

Jak zapobiegać atakom DDoS według typu

Radzenie sobie z atakami DDoS może przypominać migrenę. W jednej chwili wszystko jest w porządku, a w następnej odczuwasz cyfrowy ból. Ale zgadnij co? Nie musisz przez to cierpieć. Przeprowadzimy Cię przez różne sposoby tych ataków i, co ważniejsze, jak możesz zneutralizować każdy z nich i utrzymać płynność swojej działalności.

01

Powódź DNS

Użyj Cloudflare DNS jako głównego lub dodatkowego resolvera i włącz DNS Firewall lub Magic Transit dla dodatkowej ochrony. Globalna sieć Cloudflare filtruje zniekształcony lub nadmierny ruch DNS, jednocześnie buforując i obsługując zapytania pochodzące od legalnych użytkowników. Obsługuje dziesiątki milionów żądań DNS na sekundę, automatycznie blokując floody, zanim dotrą do źródła.

02

Powódź SYN

Wdróż Cloudflare Magic Transit, aby zatrzymać powódzie SYN na brzegu sieci. Wykorzystuje pliki cookie SYN, śledzenie połączeń i analizę zachowań, aby oddzielić prawdziwych użytkowników od sfalszowanych adresów IP lub złośliwego ruchu. Dla dodatkowej ochrony, przekieruj ruch przez Cloudflare Spectrum (dla TCP) lub Cloudflare CDN/Web Application Firewall (dla HTTP). Te odwrotne serwery proxy uniemożliwiają bezpośredni dostęp do źródła i blokują ruch DDoS oparty na protokole TCP, zanim wyrządzi on szkody.

03

Powódź UDP

Zastanawiałeś się, jak zapobiec atakowi DDoS, który wysyła ruch UDP flood? Użyj Magic Transit lub Spectrum, aby zidentyfikować i odrzucić go w czasie rzeczywistym. Połącz to z Magic Firewall, aby zastosować inteligentne ograniczenie szybkości lub całkowicie zablokować niechciane pakiety UDP, chroniąc swoją infrastrukturę przed skokami wolumetrycznymi.

04

Teeworlds

Chroń swoje serwery gier za pomocą Cloudflare Spectrum lub Magic Transit. Cloudflare automatycznie pobiera odciski palców i filtruje ruch DDoS, umożliwiając jednocześnie łączenie się prawdziwym graczom. Aby uzyskać dodatkową kontrolę, użyj Magic Firewall do tworzenia niestandardowych reguł, które zatrzymują ataki na poziomie pakietów.

05

RIPv1

Wyłącz RIPv1 na wszystkich routerach i przełącz się na RIPv2 z uwierzytelnianiem, jeśli wymagany jest routing. Zablokuj przychodzący UDP port 520 z niezaufanych sieci i monitoruj nietypową aktywność routingu, aby wcześniej wykryć potencjalne nadużycia.

06

RDP

Użyj Magic Transit, aby zablokować sfalszowany lub zniekształcony ruch RDP, zanim dotrze on do twojego źródła. Aby zabezpieczyć zdalny dostęp w warstwie aplikacji, przenieś RDP za Cloudflare Gateway lub Zero Trust Network Access (ZTNA), które wymagają uwierzytelnienia i pomagają zapobiegać nadużyciom otwartych usług RDP.

07

DemonBot

Jak chronić się przed atakami DDoS przeprowadzanymi przez DemonBot? Zwróć się do Magic Transit, który filtruje masowe powódzie w warstwach 3 i 4. Cloudflare identyfikuje zainfekowany ruch za pomocą analizy w czasie rzeczywistym i wykrywania sygnatur. W przypadku ataków w warstwie 7 użyj ochrony WAF i DDoS Cloudflare, aby zablokować powódzie HTTP i nadużywanie połączeń.

08

VxWorks Flood

Wdrożenie Magic Transit do filtrowania ruchu DDoS z zagrożonych urządzeń VxWorks. Cloudflare wykrywa i blokuje ten ruch przy użyciu niestandardowej heurystyki i odcisków palców na żywo. W celu ochrony warstwy aplikacji, połącz z usługami Cloudflare Gateway i WAF, aby bronić się przed nadużyciami na poziomie protokołu.

Nie ma zaprzeczenia: Twoja ochrona przed atakami DDoS wygrałaby z Cloudfresh!

 cloudfresh.com

 hi@cloudfresh.com