

Jak zabránit útoku DDoS podle typu

Řešení DDoS může připomínat migrénu. V jednu chvíli je všechno v pořádku, v další chvíli vás trápí digitální bolest. Ale hádejte co? Nemusíte se tím trápit. Provedeme vás různými způsoby, kterými tyto útoky zasahují, a co je důležitější, jak můžete každý z nich neutralizovat a udržet svůj byznys v chodu.

01

Zaplavení DNS

Používejte Cloudflare DNS jako primární nebo sekundární resolver a pro další ochranu zapněte bránu DNS Firewall nebo Magic Transit. Globální síť Cloudflare filtruje závadný nebo nadměrný provoz DNS a zároveň ukládá do mezipaměti a obsluhuje dotazy přicházející od legitimních uživatelů. Zpracovává desítky milionů požadavků DNS za sekundu a automaticky blokuje záplavy ještě předtím, než se dostanou k vašemu původci.

02

SYN Flood

Nasazením služby Cloudflare Magic Transit zastavíte záplavy SYN na okraji sítě. Využívá soubory cookie SYN, sledování připojení a analýzu chování k oddělení skutečných uživatelů od podvržených IP adres nebo škodlivého provozu. Pro další ochranu směrujte provoz přes Cloudflare Spectrum (pro TCP) nebo Cloudflare CDN/Web Application Firewall (pro HTTP). Tyto reverzní proxy servery zabraňují přímému přístupu k vašemu původu a blokují provoz DDoS založený na protokolu TCP dříve, než způsobí škody.

03

Záplava UDP

Přemýšleli jste, jak zabránit útoku DDoS, který odesílá v provozu UDP flood? Použijte Magic Transit nebo Spectrum k jeho identifikaci a přerušení v reálném čase. V kombinaci se službou Magic Firewall můžete použít inteligentní omezování rychlosti nebo zcela zablokovat nežádoucí pakety UDP a ochránit tak svou infrastrukturu před volumetrickými nárazy.

04

Teeworlds

Chraňte své herní servery pomocí Cloudflare Spectrum nebo Magic Transit. Cloudflare automaticky snímá otisky prstů a filtruje provoz DDoS a zároveň umožňuje připojení skutečných hráčů. Pro vyšší úroveň kontroly, použijte Magic Firewall a vytvořte vlastní pravidla, která zastaví útoky na úrovni paketů.

05

RIPv1

Vypněte RIPv1 na všech směrovačích a v případě potřeby směrování přejděte na RIPv2 s ověřováním. Blokuje příchozí port UDP 520 z nedůvěryhodných sítí a sledujte neobvyklou směrovací aktivitu, abyste včas zachytili potenciální zneužití.

06

RDP

Použijte Magic Transit k blokování podvrženého nebo chybně formulovaného provozu RDP dříve, než se dostane k vašemu původu. Chcete-li zabezpečit vzdálený přístup na aplikační vrstvě, přesuňte RDP za bránu Cloudflare nebo Zero Trust Network Access (ZTNA), které vyžadují ověření a pomáhají zabránit zneužití otevřených služeb RDP.

07

DemonBot

Jak se chránit proti DDoS, který je prováděn prostřednictvím DemonBot? Obrátte se na službu Magic Transit, která filtruje masivní záplavy na vrstvách 3 a 4. Cloudflare identifikuje infikovaný provoz pomocí analýzy v reálném čase a detekce vzorců. Pro útoky na vrstvě 7 použijte ochranu WAF a DDoS společnosti Cloudflare, která blokuje záplavy HTTP a zneužití připojení.

08

VxWorks Flood

Nasadte Magic Transit k filtrování provozu DDoS z napadených zařízení VxWorks. Cloudflare tento provoz detekuje a blokuje pomocí vlastní heuristiky a živého snímání otisků prstů. Pro ochranu na aplikační vrstvě kombinujte se službami Cloudflare Gateway a WAF, které chrání před zneužitím na úrovni protokolu.

**Neexistuje žádné odmítnutí:
Vaše ochrana proti DDoS by
se službou Cloudfresh vyhrála!**



cloudfresh.com



hi@cloudfresh.com