cloudfresh

CLOUDFLARE

How to Prevent a DDoS Attack by Type

Dealing with DDoS can feel like a migraine. One minute everything's fine, the next you're in digital pain. But guess what? You don't have to suffer through it. We'll walk you through the various ways these attacks hit and, more importantly, how you can neutralize each one and keep your business flowing.

01

DNS Flood

Use Cloudflare DNS as your primary or secondary resolver, and enable DNS Firewall or Magic Transit for added protection. Cloudflare's global network filters malformed or excessive DNS traffic while caching and serving queries coming from legitimate users. It handles tens of millions of DNS requests per second, automatically blocking floods before they reach your origin.

02

SYN Flood

Deploy Cloudflare Magic Transit to stop SYN floods at the edge. It uses SYN cookies, connection tracking, and behavioral analysis to separate real users from spoofed IP addresses or malicious traffic. For additional protection, route traffic through Cloudflare Spectrum (for TCP) or Cloudflare's CDN/Web Application Firewall (for HTTP). These reverse proxies prevent direct access to your origin and block TCP-based DDoS traffic before it causes harm.

03

UDP Flood

Been wondering how to prevent a DDoS attack that sends in UDP flood traffic? Use Magic Transit or Spectrum to identify and drop it in real time. Combine this with Magic Firewall to apply smart rate limiting or block unwanted UDP packets entirely, keeping your infrastructure protected from volumetric surges.

04

Teeworlds

Protect your game servers using Cloudflare Spectrum or Magic Transit. Cloudflare automatically fingerprints and filters out DDoS traffic while allowing real players to connect. For extra control, use Magic Firewall to craft custom rules that stop attacks at the packet level.

05

RIPv1

Disable RIPv1 on all routers and switch to RIPv2 with authentication if routing is required. Block inbound UDP port 520 from untrusted networks and monitor for unusual routing activity to catch potential abuse early.

06

RDP

Use Magic Transit to block spoofed or malformed RDP traffic before it hits your origin. To secure remote access at the application layer, move RDP behind Cloudflare Gateway or Zero Trust Network Access (ZTNA), which require authentication and help prevent abuse of open RDP services.

07

DemonBot

How to protect against DDoS that's carried out via DemonBot? Turn to Magic Transit, which filters massive floods at layers 3 and 4. Cloudflare identifies infected traffic using real-time analysis and signature detection. For Layer 7 attacks, use Cloudflare's WAF and DDoS protection to block HTTP floods and connection abuse.

08

VxWorks Flood

Deploy Magic Transit to filter DDoS traffic from compromised VxWorks devices. Cloudflare detects and blocks this traffic using custom heuristics and live fingerprinting. For application-layer protection, combine with Cloudflare Gateway and WAF services to defend against protocol-level abuse.

There's no Denial: Your DDoS Protection Would Win with Cloudfresh!

cloudfresh.com

hi@cloudfresh.com