cloudfresh CLOUDFLARE

Comment prévenir une attaque DDoS par type

Faire face à une attaque DDoS, c'est comme subir une migraine soudaine : tout va bien, puis tout s'écroule. Mais bonne nouvelle ! Vous pouvez éviter la douleur. Voici les principaux types d'attaques et comment les neutraliser efficacement.

01

Inondation DNS

Utilisez Cloudflare DNS comme résolveur principal ou secondaire, et activez DNS Firewall ou Magic Transit pour renforcer la protection. Le réseau mondial de Cloudflare filtre le trafic DNS malformé ou excessif, tout en mettant en cache et en distribuant les requêtes des utilisateurs légitimes. Capable de traiter des dizaines de millions de requêtes DNS par seconde, il bloque automatiquement les inondations avant qu'elles ne parviennent à votre serveur d'origine.

02

Inondation SYN

Déployez Cloudflare Magic Transit pour stopper les inondations SYN dès la périphérie, en utilisant des cookies SYN, le suivi des connexions et l'analyse comportementale afin de distinguer le trafic légitime des adresses IP usurpées ou malveillantes. Pour une protection renforcée, faites transiter le trafic par Cloudflare Spectrum (pour TCP) ou par Cloudflare CDN et Web Application Firewall (pour HTTP). Ces proxys inversés empêchent l'accès direct à votre serveur et bloquent le trafic DDoS basé sur TCP avant qu'il ne cause des dommages.

03

Inondation UDP

Pour bloquer une attaque DDoS par inondation UDP, appuyez-vous sur Magic Transit ou Spectrum, capables de l'identifier et de l'éliminer en temps réel. En complément, Magic Firewall permet d'appliquer une limitation intelligente du débit ou de bloquer entièrement les paquets UDP indésirables, préservant ainsi vos systèmes des surcharges massives.

04

Teeworlds

Protégez vos serveurs de jeu grâce à Cloudflare Spectrum ou Magic Transit, qui identifient et filtrent automatiquement le trafic DDoS, tout en laissant passer les vrais joueurs. Pour un contrôle plus poussé, utilisez Magic Firewall afin de définir des règles personnalisées qui stoppent les attaques au niveau des paquets.

05

RIPv1

Désactivez RIPv1 sur tous vos routeurs et migrez vers RIPv2 avec authentification si le routage est nécessaire. Bloquez le port UDP 520 entrant depuis des réseaux non fiables et surveillez toute activité de routage inhabituelle afin de repérer rapidement d'éventuels abus.

06

RDP

Utilisez Magic Transit pour bloquer le trafic RDP usurpé ou malformé avant qu'il n'atteigne votre serveur. Pour sécuriser l'accès distant au niveau applicatif, placez le RDP derrière Cloudflare Gateway ou Zero Trust Network Access (ZTNA), qui imposent une authentification stricte et limitent les risques liés aux services RDP exposés.

07

DemonBot

Pour contrer les attaques menées par DemonBot, déployez Magic Transit, qui filtre les inondations massives aux niveaux 3 et 4 grâce à une analyse en temps réel et à la reconnaissance des signatures. Pour la couche 7, le Web Application Firewall et la protection DDoS Cloudflare bloquent efficacement les inondations HTTP et les abus de connexion.

08

VxWorks Flood

Mettez en place Magic Transit pour bloquer le trafic DDoS issu d'appareils VxWorks compromis. Cloudflare utilise une heuristique dédiée et une empreinte digitale en direct pour détecter et filtrer ce type de menace. Pour protéger la couche applicative, associez Cloudflare Gateway aux services WAF afin de contrer les abus au niveau protocolaire.

C'est indéniable : votre protection DDoS se portera mieux que jamais avec Cloudfresh!

cloudfresh.com

hi@cloudfresh.com