GABRIELE ROMANATO

Le funzionalità anti-DoS di Cloudflare

Con l'aumento della connettività globale e della presenza online, le minacce informatiche sono diventate sempre più sofisticate. Tra queste, gli attacchi DoS (Denial of Service) e DDoS (Distributed Denial of Service) sono tra le più diffuse. Cloudflare, un'azienda leader nel settore della sicurezza informatica e della performance online, ha sviluppato una serie di funzionalità specifiche per contrastare tali minacce. In questo articolo esploreremo come Cloudflare protegge i siti web dagli attacchi DoS e DDoS, analizzando le sue principali tecnologie e strategie di difesa.

Che Cos'è un Attacco DoS e DDoS?

Un attacco DoS mira a rendere un servizio o un sito web non disponibile agli utenti legittimi, sovraccaricando il server con una quantità eccessiva di richieste, fino al punto in cui non può più rispondere. Un DDoS è una versione distribuita di questo tipo di attacco, dove migliaia o milioni di dispositivi compromessi (botnet) sono utilizzati per generare traffico verso l'obiettivo, rendendo molto più difficile bloccare le fonti del traffico malevolo.

Cloudflare: Una Difesa Completa contro gli Attacchi DDoS

Cloudflare offre una protezione multi-livello contro gli attacchi DoS e DDoS, sfruttando una combinazione di tecnologie avanzate, un'infrastruttura globale e algoritmi di rilevamento intelligente. Ecco come funziona:

1. Infrastruttura Globale di Rete Distribuita

Cloudflare gestisce una delle reti più grandi del mondo, con data center presenti in oltre 275 città a livello globale. Questo permette all’azienda di

assorbire e distribuire grandi volumi di traffico, che potrebbero provenire da attacchi DDoS, su una rete molto vasta. L'idea alla base di questo approccio è che un attacco DDoS, per essere efficace, deve superare la capacità di banda disponibile. Con la vasta rete di Cloudflare, anche gli attacchi più grandi possono essere gestiti distribuendo il traffico su più server.

2. Mitigazione Automatizzata degli Attacchi DDoS

Una delle caratteristiche più potenti di Cloudflare è la sua capacità di rilevare automaticamente un attacco DDoS e mitigarlo senza l'intervento umano. Grazie all'uso di algoritmi avanzati di machine learning, Cloudflare può analizzare il traffico in tempo reale e distinguere tra il traffico legittimo e quello malevolo. Quando viene identificato un attacco, Cloudflare attiva automaticamente meccanismi di mitigazione che filtrano il traffico in modo che solo le richieste legittime arrivino al server target.

3. Rate Limiting

Una delle tecniche più efficaci contro gli attacchi DoS di tipo volumetrico è il *rate limiting*. Questa funzione consente di limitare il numero di richieste che un utente può inviare a un server in un determinato periodo di tempo. Se un IP o un insieme di IP supera il limite stabilito, il traffico viene bloccato o rallentato. Questo è particolarmente utile per prevenire attacchi che cercano di sopraffare i server con una quantità eccessiva di richieste HTTP o altre forme di richieste di servizio.

4. Anycast Routing

L'infrastruttura di Cloudflare utilizza un sistema di *anycast routing*, il quale consente di instradare il traffico dell'attacco verso il nodo Cloudflare più vicino all'origine dell'attacco stesso. Questo riduce il carico sui server di destinazione e permette a Cloudflare di mitigare l’attacco in modo più efficiente, sfruttando la capacità della sua rete globale.

5. Firewall di Applicazioni Web (WAF)

Il *Web Application Firewall* di Cloudflare è un'altra linea di difesa contro gli attacchi DDoS. Il WAF protegge specificamente le applicazioni web da attacchi che cercano di sfruttare vulnerabilità nel codice dell’applicazione o di inviare richieste HTTP dannose. Può bloccare pattern specifici di attacchi, come iniezioni SQL, attacchi XSS (cross-site scripting) e altre minacce comuni per le applicazioni web.

6. Protezione DNS e Proxy Inverso

Cloudflare funziona anche come un proxy inverso, nascondendo l'indirizzo IP reale del server dietro i propri server proxy. Questo rende più difficile per gli attaccanti individuare l'indirizzo IP del server per lanciare un attacco diretto. Inoltre, Cloudflare offre protezione contro attacchi mirati al DNS, proteggendo la risoluzione dei nomi di dominio da attacchi come il DNS flood, che potrebbe rendere un sito web inaccessibile agli utenti.

7. Modalità "Under Attack"

Per i casi di attacchi estremamente gravi, Cloudflare offre una modalità speciale chiamata *Under Attack Mode*. Quando abilitata, questa modalità applica controlli di sicurezza aggiuntivi su tutte le richieste in ingresso, come l'uso di CAPTCHA per verificare se un visitatore è un utente umano o parte di un attacco botnet. Sebbene questo possa rallentare leggermente l'accesso legittimo al sito, è estremamente efficace nel prevenire il sovraccarico causato da attacchi DDoS su larga scala.

8. Protezione Livello 7 (Layer 7)

Gli attacchi a livello applicativo (Layer 7) sono tra i più complessi, poiché mirano a sovraccaricare il livello di applicazione (ad esempio HTTP, HTTPS) del server. Cloudflare protegge da questi attacchi distinguendo il traffico umano dal traffico bot e blocca automaticamente le richieste che

mostrano comportamenti anomali, come l'accesso rapido a molte pagine in un breve periodo di tempo.

Conclusione

La protezione contro gli attacchi DoS e DDoS è cruciale per qualsiasi sito web o servizio online. Cloudflare, con la sua vasta infrastruttura distribuita, le tecnologie di mitigazione automatizzate e le funzionalità di sicurezza avanzate come il rate limiting e il WAF, offre una delle soluzioni più efficaci e complete per difendersi da questi attacchi. Grazie alla sua capacità di assorbire grandi volumi di traffico e distinguere rapidamente tra utenti legittimi e malevoli, Cloudflare è una scelta ideale per chi cerca protezione avanzata e affidabile contro una delle minacce più persistenti del web.