WHITEPAPER

Ottimizza le prestazioni e la sicurezza dei siti Web in Cina

Strategie per attingere all'economia di Internet massiccia, complessa e in rapida crescita della Cina

+44 20 3514 6970 | enterprise@cloudflare.com | www.cloudflare.com/it-it/

Riepilogo

La Cina ospita la più grande popolazione mondiale connessa a Internet. Tuttavia, la complessità della rete e la minaccia sempre presente degli attacchi informatici possono rendere difficile l'accesso a questo mercato. Per aiutare le organizzazioni a superare questi ostacoli e ottimizzare al meglio l'esperienza del loro sito Web per gli utenti in Cina, Cloudflare ha esteso senza soluzione di continuità le sue prestazioni globali e i servizi di rete di sicurezza in Cina.

I problemi legati all'espansione di un business online in Cina

La vasta economia online della Cina in rapida crescita la rende un mercato interessante per una varietà di aziende. Oltre un miliardo di cittadini cinesi è connesso a Internet , la più grande popolazione mondiale connessa a Internet, e oltre 812 milioni di queste persone hanno effettuato almeno un acquisto online nella prima metà del 2021. La spesa online complessiva è leggermente diminuita durante quel periodo rispetto agli anni precedenti, in gran parte a causa della più ampia instabilità economica causata dalla pandemia di Covid-19, ma l'economia cinese ha ancora registrato una crescita a doppia cifra nel post-Covid, mentre il mercato dell'e-commerce è cresciuto del 12,5% nel 2020.

Come per qualsiasi mercato regionale, le aziende globali che operano in Cina devono adattare i propri servizi e le proprie esperienze online per soddisfare le aspettative locali. Sfortunatamente, le normative Internet cinesi, l'infrastruttura sottostante e il panorama delle minacce presentano una serie di problemi unici che possono rendere più difficile per le aziende globali fornire la qualità dell'esperienza che i consumatori locali si aspettano. Tali problemi includono:

- Latenza causata da reti frammentate e peering locale scadente
- Compromessi delle prestazioni del sito Web mobile
- Attacchi informatici nazionali persistenti

Questo documento descrive questi problemi in dettaglio, descrive le strategie per risolverli e mostra come Cloudflare può aiutare.

Latenza causata da colli di bottiglia di Internet e peering locale scadente

Come molti consumatori, le persone in Cina hanno grandi aspettative per le esperienze online. Sulla base del rapporto di HSBC, la Cina è leader e domina il mercato dell'e-commerce in tutto il mondo, identificato come il più grande mercato di e-commerce del mondo per paese dall'analisi di business.com.

Sfortunatamente, le organizzazioni spesso faticano a far funzionare i loro siti in modo rapido e affidabile per gli utenti in Cina.

Uno dei motivi sono i colli di bottiglia della rete. Tutto il traffico Internet in entrata e in uscita dalla Cina passa attraverso uno dei tre Internet Exchange Point (IXP): a Pechino, Shanghai o Guangzhou. Durante i periodi di utilizzo elevato, questi IXP possono diventare congestionati e aumentare significativamente i tempi di caricamento dei siti Web ospitati al di fuori della Cina. Una serie di test ha rilevato che il sito Web TED ha impiegato dagli 8 ai 38 secondi per caricarsi per la prima volta a Shanghai durante un periodo di picco di navigazione, rispetto a un intervallo da 5 a 8 secondi a New York durante un periodo comparabile.

Per evitare questi colli di bottiglia, alcune aziende globali scelgono di ospitare i propri siti Web in datacenter vicino a uno dei tre IXP cinesi, ad esempio a Hong Kong per essere vicini all'IXP di Guangzhou o su server entro i confini cinesi. Tuttavia, questi approcci sono ancora a rischio a causa di un altro importante problema di rete: un numero limitato di provider di servizi Internet (ISP) locali con un peering scadente.

Le aziende che hanno familiarità con il panorama Internet cinese potrebbero già sapere che tre ISP statali dominano il mercato: China Telecom, China Mobile e China Unicom. Ciascuno di questi ISP domina in una determinata parte del paese. Si impegnano anche in un peering relativamente ridotto o nella pratica di collegare reti separate agli IXP. Uno studio di MIytics del 2017 ha rilevato che la rete con più peering in Cina era connessa solo a due IXP, rispetto a 66 in Nord America e 71 in Europa.

Ciò significa che anche il traffico Internet nazionale spesso deve coprire una grossa quantità di distanza di rete per percorrere una distanza geografica relativamente breve, con conseguente latenza aggiuntiva per gli utenti finali.

Come superare i colli di bottiglia e il peering locale scadente

Di fronte a queste sfide relative alle prestazioni Web, molte organizzazioni globali che operano in Cina scelgono di utilizzare una rete di distribuzione dei contenuti (CDN) per memorizzare nella cache i contenuti di siti Web statici (o non specifici dell'utente) nei datacenter vicini agli utenti finali, in modo che molti le loro richieste non devono tornare indietro fino a un server di origine. Le organizzazioni dovrebbero considerare CDN che:

- **Avere una rete ampia e con un buon peering**. Più datacenter ha una CDN, più sarà vicina agli utenti finali. E migliore è la copertura dei tre principali ISP cinesi, meno salti di rete dovranno essere richiesti dagli utenti finali.
- **Possono risolvere query DNS all'interno dei confini cinesi.** Il processo di risoluzione DNS, il processo mediante il quale i nomi di dominio vengono convertiti in indirizzi IP, può aggiungere latenza se il suo traffico deve viaggiare dentro e fuori la Cina, anche se altri contenuti del sito sono memorizzati nella cache locale.
- **Minimizzazione del codice HTML, CSS e Javascript dei siti Web.** Questi tipi di codice sono gli elementi costitutivi della maggior parte dei siti Web e indicano ai browser degli utenti finali come dovrebbe essere il sito. La minimizzazione è il processo di rimozione dei caratteri non necessari dal codice, riducendone le dimensioni complessive e facendo così occupare meno larghezza di banda durante l'attraversamento di una rete. Una larghezza di banda inferiore implica che il sito si carica più velocemente.
- **Utilizzare codice serverless sul perimetro di rete per creare regole personalizzate per rispondere alle richieste.** Il codice serverless è un codice che non è confinato a un determinato server controllato da uno sviluppatore. Quando viene eseguito sul perimetro di rete, il codice serverless esiste in una vasta rete di datacenter. Ciò significa che il codice può applicare in modo semplice e rapido regole speciali al traffico specifico dell'utente finale. Ad esempio, un'organizzazione potrebbe scrivere codice serverless su una rete con sede in Cina che applica regole speciali per utenti mobili, connessioni Internet più lente e molti altri casi d'uso.

La partnership di rete di Cloudflare con JD Cloud, insieme ai nostri servizi di prestazioni globali, può aiutare a superare sia i colli di bottiglia del traffico che il peering scadente. Vai alla sezione successiva di questo documento per vedere come.

Attacchi informatici nazionali persistenti

Come in qualsiasi regione, i siti Web che operano in Cina devono affrontare una serie di minacce alla sicurezza.

Una di queste minacce è data dagli attacchi DDoS (Distributed Denial-of-Service), che bombardano i server o l'infrastruttura di rete con così tanto traffico spazzatura da non essere in grado di rispondere a richieste legittime. Un report del 2017 di Talos Intelligence ha rilevato che i servizi DDoS domestici a noleggio, che consentono agli utenti non esperti di lanciare facilmente attacchi utilizzando una botnet esistente di dispositivi infetti, si stavano espandendo rapidamente in Cina.

Da quel momento, le forze dell'ordine cinesi hanno chiuso diverse importanti botnet DDoS, inclusa una nel 2019 che aveva infettato oltre 200.000 dispositivi e lanciato attacchi fino a 200 Gbps. Ma altre botnet sono ancora attive, come ad esempio DoubleGuns, i cui operatori sono ancora in libertà al momento della pubblicazione di questo documento.

I siti Web in Cina devono anche impedire i tentativi di accesso ai dati privati e agli ambienti di sviluppo. Nel 2018, gli autori di attacchi hanno sfruttato una vulnerabilità in un popolare framework PHP nel tentativo di accedere ai server di oltre 45.000 siti web cinesi. Gli attacchi al framework sono iniziati meno di 24 ore dopo la pubblicazione della sua vulnerabilità. Allo stesso modo, nel 2020, due aggressori con sede in Cina sono stati incriminati per aver accesso illegalmente alle reti private di centinaia di aziende nel corso di dieci anni, sempre sfruttando una serie di vulnerabilità delle applicazioni Web.

Inoltre, le organizzazioni che vogliono proteggere i dati privati in Cina potrebbero non essere in grado di utilizzare il loro solito toolkit. Senza moderni standard di crittografia come TLS 1.3 e Encrypted Server Name Identification (ESNI) nelle reti cinesi, crea maggiori possibilità per osservatori non autorizzati di spiare il traffico.

Come difendersi dai persistenti attacchi informatici nazionali in Cina

L'aumento degli attacchi DDoS in tutto il mondo ha reso i servizi di mitigazione DDoS — e altri strumenti per la sicurezza delle applicazioni come i firewall delle applicazioni Web (WAF) — una tabella dei requisiti di sicurezza per qualsiasi sito Web attivo. La Cina non è diversa. Quando cercano tale protezione in questo mercato, le organizzazioni dovrebbero prendere in considerazione:

- **Mitigazione DDoS dal perimetro della rete piuttosto che "scrubbing center" limitati.** Sebbene quasi tutti i moderni servizi di mitigazione DDoS operino nel cloud, molti si affidano a un numero limitato di datacenter per filtrare o eseguire lo "scrubbing" del traffico dannoso. Il backhauling del traffico verso questi "scrubbing center" per l'ispezione può richiedere ulteriori salti di rete e quindi causare latenza e interruzioni agli utenti soprattutto in Cina, con i suoi limiti di rete. Per fornire la mitigazione DDoS senza influire sulle prestazioni Internet in Cina, le organizzazioni dovrebbero prendere in considerazione i servizi cloud che offrono la mitigazione degli DDoS in ogni datacenter perimetrale senza aggiungere ulteriori salti di rete.
- **Limitazione della frequenza per bloccare l'abuso.** È essenziale disporre di controlli granulari in grado di mitigare gli attacchi DDoS di livello 7 ad alta precisione, fermare gli abusi delle API per garantire la disponibilità, proteggere le informazioni sensibili dei clienti da attacchi di accesso brutale e proteggere i server di origine dall'esaurimento delle risorse, il tutto evitando costi imprevedibili dovuti al traffico picchi.

- **WAF che si aggiornano automaticamente e rapidamente.** Gli autori di attacchi nazionali in Cina si sono dimostrati in grado di sfruttare molto rapidamente le nuove vulnerabilità delle applicazioni Web. Le organizzazioni potrebbero voler creare le proprie regole WAF, ma non dovrebbero fare affidamento esclusivamente sulla propria intelligence sulle minacce e sulla capacità di effettuare aggiornamenti. Dovrebbero prendere in considerazione i firewall delle applicazioni Web che si aggiornano automaticamente in base a un ampio pool di minacce osservate. E quando l'organizzazione desidera apportare i propri aggiornamenti alle regole, dovrebbe essere sicura che tali modifiche si propagheranno il più rapidamente possibile.
- **Opzioni di crittografia personalizzabili.** Per proteggere i dati in transito in assenza di TLS 1.3 ed ESNI, le organizzazioni dovrebbero prendere in considerazione servizi di sicurezza che offrano una gamma più ampia di metodi di crittografia personalizzabili.

I servizi di sicurezza di Cloudflare, disponibili come parte della nostra rete cinese, offrono mitigazione DDoS senza latenza e un WAF a rapido aggiornamento che attinge dall'intelligence globale sulle minacce. Vai alla sezione successiva di questo documento per saperne di più.

In che modo Cloudflare supporta i siti Web globali che operano in Cina

Cloudflare gestisce una rete di data center che copre 200 città globali in 100 paesi. In Cina, a marzo 2022, c'erano 45 datacenter distribuiti in 38 città. Ciascuno di questi datacenter può eseguire un'ampia gamma di servizi di sicurezza, prestazioni e affidabilità, tra cui distribuzione di contenuti, risoluzione DNS, mitigazione DDoS, applicazione WAF, esecuzione di codice serverless e molto altro. Poiché ciascuno di questi servizi opera in ogni singolo datacenter, possono funzionare molto vicino agli utenti finali contribuendo a ridurre la latenza e fornendo alla nostra rete una visione dettagliata e aggiornata delle ultime minacce e condizioni di rete. Inoltre, le organizzazioni possono gestire tutti questi servizi da un unico dashboard.

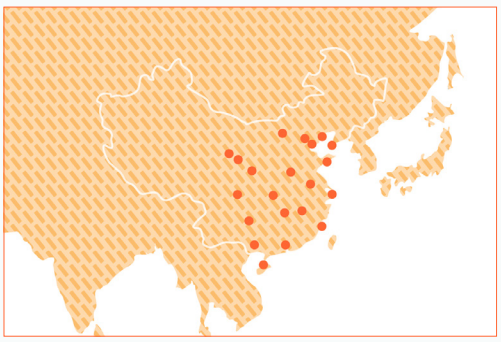
Dal 2015 Cloudflare aiuta le organizzazioni a offrire un'esperienza Internet sicura, veloce e affidabile per i visitatori con sede in Cina. Al fine di migliorare ulteriormente questi servizi, abbiamo recentemente avviato una partnership con JD Cloud, la business unit cloud e tecnologia intelligente del colosso cinese di Internet JD.com.

Ecco come questa rete aiuterà le organizzazioni a risolvere i problemi descritti nella sezione precedente.

In che modo Cloudflare aiuta a superare la latenza

La rete di Cloudflare e JD Cloud in Cina offre:

- **Argo Smart Routing:** La trasmissione di dati dal client all'origine e viceversa può introdurre latenza. Con la memorizzazione nella cache, il contenuto statico può evitare la congestione della rete, ma il contenuto dinamico si basa sulla disponibilità, l'affidabilità e le prestazioni di Internet. Ciò può portare a tempi di caricamento lenti, timeout, disconnessioni e un'esperienza dell'utente finale degradata. **Argo Smart Routing** ha la possibilità di **rilevare le congestioni in tempo reale** e **instradare il traffico Web**verso i **percorsi di rete più veloci ed affidabili**. Le richieste alla rete di Cloudflare da parte dei clienti di Cloudflare e dei loro utenti ci aiutano a capire le prestazioni delle diverse parti di Internet in un dato momento. Argo Smart Routing utilizza i dati temporali raccolti da Cloudflare per **instradare dinamicamente il traffico lungo i percorsi più veloci verso l'origine**, aumentando in questo modo le prestazioni. In media, Argo migliora le prestazioni delle risorse Web di circa il 30%, portando successivamente a un aumento delle vendite e della fidelizzazione dei clienti.
- **Caching e pubblicazione di contenuto statico da molti datacenter all'interno della Cina**, offrendo una latenza inferiore e tempi di caricamento delle pagine più rapidi indipendentemente da dove si trovano gli utenti finali. La nostra rete è strettamente interconnessa con tutti gli ISP cinesi, riducendo il numero di salti di rete necessari al traffico.



Datacenter nella Cina continentale

- **Risoluzione DNS opzionale all'interno della Cina**, di nuovo con conseguente tempi di risposta più rapidi.
- La possibilità di **utilizzare Internet Protocol versione 6** (IPv6), che consente routing ed elaborazione dei pacchetti efficienti.
- La possibilità di **minimizzare il codice dei siti Web** tramite la nostra funzionalità Auto Minify, che può essere facilmente attivata selezionando una casella nel dashboard di Cloudflare.
- **Elaborazione serverless** tramite il servizio Cloudflare Workers, che opera in tutti i datacenter della nostra rete cinese. Ti consente di rispondere a determinate richieste in modi personalizzabili, aumentare le applicazioni esistenti. E anche crearne di completamente nuovi senza configurare o mantenere l'infrastruttura.

In che modo Cloudflare aiuta a gestire gli attacchi informatici nazionali persistenti

I servizi di sicurezza integrati nella nostra rete cinese consentono alle organizzazioni di:

- **Mitigare gli attacchi DDoS.** Ciascuno dei nostri datacenter in Cina può mitigare gli attacchi, fornendo alla rete un'immensa capacità di assorbire gli attacchi più grandi senza perdere le richieste legittime e senza fare affidamento sui data center Cloudflare in altre parti del mondo. Poiché l'ispezione del traffico avviene vicino agli utenti finali, alle loro richieste viene risparmiato il lungo processo di trasferimento a uno "scrubbing center" potenzialmente distante. E a causa dei problemi di rete in Cina, Cloudflare offre funzionalità esclusive di ingegneria del traffico automatizzate che consentono il reindirizzamento automatico del traffico d'attacco. Tutte queste funzionalità prevengono le penalità delle prestazioni per il traffico legittimo all'interno e all'esterno della Cina.
- **Proteggere le vulnerabilità delle applicazioni Web** con Cloudflare WAF. Oltre a bloccare i vettori di attacco noti grazie a set di regole gestiti (come un'implementazione di OWASP e regole proprietarie di Cloudflare), il WAF attinge a un flusso continuo di informazioni sulle minacce da tutta la nostra rete per fermare automaticamente le minacce più recenti. Inoltre, le organizzazioni possono creare facilmente le proprie regole e diffonderle sull'intera rete in pochi minuti. I miglioramenti apportati nel 2021 consentono a WAF di essere implementato più rapidamente e di scalare facilmente per coprire ancora più traffico. WAF ha anche set di regole aggiornati che forniscono un migliore controllo separando lo stato delle regole dall'azione. Gli utenti possono ora godere di una migliore navigazione delle regole attraverso filtri avanzati, modifiche in blocco, tag delle regole e così via.
- La **limitazione della frequenza** è integrata con le nostre regole personalizzate WAF e protegge da attacchi DDoS, tentativi di accesso a forza bruta, sovraccarico del server di origine e altri tipi di abusi che prendono di mira API e applicazioni. Gli utenti possono configurare soglie, definire il traffico, personalizzare le risposte e ottenere informazioni preziose su URL specifici di siti Web, applicazioni o endpoint API.
- **Crittografare i dati tramite TLS 1.2** e gestire facilmente le certificazioni dal dashboard di Cloudflare.

ULTERIORI INFORMAZIONI

China Network Service di Cloudflare è disponibile per tutti i clienti Enterprise di Cloudflare. Ed è pienamente conforme alle leggi e ai regolamenti cinesi, in cui una licenza ICP (Internet Content Provider) valida è un requisito obbligatorio per l'onboarding della rete cinese.

Poiché l'economia cinese di Internet continua a crescere, emergeranno inevitabilmente nuovi problemi in termini di sicurezza e prestazioni. I piani di Cloudflare per una crescita continua in Cina consentono alle aziende della nostra rete di rispondere rapidamente a queste sfide e continuare ad alzare il livello per un'esperienza utente senza interruzioni.

Chiama Cloudflare per iniziare a ottimizzare la tua presenza sul Web in Cina oggi stesso!

Per ulteriori informazioni su Cloudflare China Network, visitacloudflare.com/it-it/china-network/ o contatta un rappresentante Cloudflare.