ARTIGO TÉCNICO

Otimize a performance e a segurança de sites na China

Estratégias para explorar a economia da internet enorme, complexa e em rápido crescimento da China

+55 11 3230 4523 | enterprise@cloudflare.com | www.cloudflare.com/pt-br/

Sumário executivo

A China é o lar da maior população conectada à internet em todo o mundo. Entretanto, explorar esse mercado pode ser difícil com a complexidade da rede e a ameaça constante de ataques cibernéticos. Para ajudar organizações a superarem esses obstáculos e a otimizar a experiência dos usuários em sites na China, a Cloudflare ampliou os serviços globais de performance e segurança de rede de modo a incluir o país asiático.

Desafios de expandir um negócio on-line para a China

Uma economia on-line gigantesca e de rápido crescimento torna a China um mercado atrativo para vários negócios. Mais de um bilhão de cidadãos do país estão conectados à internet — a maior população conectada à internet do mundo — e mais de 812 milhões de pessoas fizeram uma compra on-line no primeiro semestre de 2021. Em geral, o gasto on-line teve uma pequena queda durante esse período em comparação com os anos anteriores, devido em grande parte à maior instabilidade econômica causada pela pandemia de COVID-19 — mas muitos setores ainda mostraram crescimento de dois dígitos após a COVID-19 e o mercado de comércio eletrônico expandiu 12,5% em 2020.

Assim como em qualquer mercado regional, as empresas globais que atuam na China precisam adaptar seus serviços e experiências virtuais para atender às expectativas locais. Infelizmente, os regulamentos de internet, a infraestrutura de base e o panorama de ameaças na China criam diversos desafios únicos que tornam difícil para uma empresa global oferecer a qualidade de experiência esperada pelos consumidores locais. Alguns desses desafios:

- Latência causada por redes fragmentadas e peering local ruim
- Perdas de performance em sites para dispositivos móveis
- Ataques cibernéticos domésticos contínuos

Este documento explica esses desafios em detalhes, descreve estratégias para superá-los e mostra como a Cloudflare pode ajudar.

Latência causada por gargalos na internet e peering local ruim

Assim como muitos consumidores, os chineses têm altas expectativas para experiências on-line. Com base no relatório do HSBC, a China lidera e domina o mercado de comércio eletrônico em todo o mundo. Além disso, é considerada um dos maiores mercados de comércio eletrônico no mundo por país de acordo com a análise do site business.com.

Infelizmente, as organizações muitas vezes têm dificuldades para fazer com que seus sites tenham uma performance rápida e confiável para usuários na China.

Um dos motivos são os gargalos na rede. Todo o tráfego da internet que entra e sai da China passa por um de três pontos de troca de tráfego da internet (IXPs): Beijing, Shanghai ou Guangzhou. Durante períodos de uso elevado, esses IXPs podem ficar congestionados e aumentar consideravelmente o tempo de carregamento de sites hospedados fora do país. Uma série de testes descobriu que o site do TED levava entre 8 e 38 segundos para carregar pela primeira vez em Shanghai durante um pico de navegação, em comparação com um intervalo de 5 a 8 segundos em Nova York em uma situação semelhante.

Para evitar esses gargalos, algumas empresas globais optam por hospedar sites em data centers próximos a um dos três IXPs da China — por exemplo, Hong Kong está perto do IXP de Guangzhou — ou em servidores dentro das fronteiras da China. No entanto, essas abordagens ainda estão em risco por conta de outro grande desafio de rede: o número limitado de provedores de internet (ISPs) locais com peering ruim.

Empresas que conhecem o cenário da internet na China já sabem que três provedores estatais dominam o mercado: China Telecom, China Mobile e China Unicom. Cada um tem controle em uma determinada parte do país e, comparativamente, envolvem-se pouco em peering, ou a prática de conectar redes separadas em IXPs. Um estudo da Mlytics de 2017 descobriu que a rede com mais troca de tráfego da China estava conectada apenas a dois IXPs, em comparação com 66 na América do Norte e 71 na Europa.

Isso significa que mesmo o tráfego da internet doméstico muitas vezes cobre uma grande quantidade de distância na Rede para percorrer uma distância geográfica relativamente curta, o que aumenta a latência para os usuários finais.

Como eliminar gargalos e peering local ruim

Diante desses desafios de performance na web, muitas organizações globais que fazem negócios na China optam por usar uma rede de distribuição de conteúdo (CDN) para armazenar em cache o conteúdo estático de sites (ou não específico do usuário) em data centers próximos aos usuários finais, para que as solicitações não precisem ser enviadas de volta a um servidor de origem. As organizações devem considerar as CNDs que:

- **Têm uma rede grande e um bom peering**. Quanto mais data centers uma CDN tiver, mais perto ela estará dos usuários finais. E quanto melhor a cobertura dos três principais provedores da China, menos saltos de rede as solicitações dos usuários finais terão que fazer.
- **Podem resolver consultas de DNS na China.** O processo de resolução de DNS — o processo pelo qual os nomes de domínio são convertidos em endereços de IP — poderá aumentar a latência se o tráfego precisar entrar e sair da China, mesmo que outro conteúdo do site esteja armazenado em cache localmente.
- **Minimizam o código HTML, CSS e Javascript do site.** Esses tipos de código são a base da maioria dos sites, pois informam aos navegadores dos usuários finais como deve ser a aparência do site. A minificação é o processo de remoção de caracteres desnecessários do código, reduzindo seu tamanho geral e, assim, fazendo com que ele ocupe menos largura de banda ao atravessar uma rede. Menos largura de banda significa que o site carrega mais rápido.
- **Usam código sem servidor na borda de rede a fim de criar regras personalizadas para responder a solicitações.** Código sem servidor é um código que não está confinado em um servidor específico controlado por um desenvolvedor. Quando executado na borda de rede, o código sem servidor fica em uma grande rede de data centers. Isso significa que o código pode aplicar regras especiais com facilidade e rapidez ao tráfego específico do usuário final. Por exemplo, uma organização poderia escrever código sem servidor em uma rede baseada na China que impõe regras especiais para usuários de dispositivos móveis, para conexões com a internet mais lentas e muitos outros casos de uso.

A parceria da Rede da Cloudflare com a JD Cloud, junto com nossos serviços globais de performance, pode ajudar a eliminar gargalos de tráfego e peering ruim. Veja como na próxima seção deste documento.

Ataques cibernéticos domésticos contínuos

Como em qualquer região, sites presentes na China enfrentam uma variedade de ameaças à segurança.

Uma dessas ameaças são os ataques de negação de serviço distribuída (DDoS), que bombardeiam servidores ou infraestrutura de rede com tanto tráfego de lixo eletrônico que fica impossível responder a solicitações legítimas. Um relatório de 2017 da Talos Intelligence descobriu que os serviços de aluguel de DDoS — que permitem a usuários não especializados iniciarem ataques facilmente usando uma botnet de dispositivos infectados — estavam se expandindo rapidamente na China.

Desde então, as autoridades policiais chinesas encerraram várias grandes botnets de DDoS, incluindo uma em 2019 que infectou mais de 200 mil dispositivos e fez ataques de até 200 Gbps. Mas outras botnets ainda estão ativas — como a DoubleGuns, cujos operadores ainda estavam foragidos no momento da publicação deste documento.

Os sites na China também precisam evitar tentativas de acessar dados privados e ambientes de desenvolvimento. Em 2018, invasores exploraram uma vulnerabilidade em um framework PHP popular na tentativa de acessar os servidores de mais de 45 mil sites chineses. Os ataques à estrutura começaram menos de 24 horas após a divulgação da vulnerabilidade. Da mesma forma, em 2020, dois invasores da China foram indiciados por acessar ilegalmente centenas de redes corporativas privadas ao longo de dez anos, novamente aproveitando uma variedade de vulnerabilidades de aplicativos web.

Além disso, as organizações que desejam proteger dados privados na China talvez não consigam usar o kit de ferramentas normal. Sem os padrões modernos de criptografia como TLS 1.3 e Encrypted Server Name Identification (ESNI), há mais chances de observadores não autorizados espionarem o tráfego.

Como se defender de ataques cibernéticos domésticos persistentes na China

O aumento nos ataques DDoS em todo o mundo tornaram os serviços de mitigação de DDoS — e outras ferramentas de segurança de aplicativos, como firewalls de aplicativos web (WAFs) — um requisito de segurança fundamental para qualquer site ativo. Na China não é diferente. Ao procurar essa proteção nesse mercado, as organizações devem considerar:

- **Mitigação de DDoS na borda da rede, em vez de "centros de depuração" limitados.** Embora quase todos os serviços modernos de mitigação de DDoS operem na nuvem, muitos dependem de um número limitado de data centers para filtrar ou "depurar" o tráfego malicioso. O backhauling do tráfego para esses "centros de depuração" para inspeção pode exigir saltos de rede extras e, assim, causar latência e interrupção para os usuários, especialmente na China, com suas limitações de rede. Para fornecer mitigação de DDoS sem afetar a performance da internet na China, as organizações devem considerar os serviços em nuvem que oferecem a mitigação de DDoS em cada data center de borda sem adicionar mais saltos de rede.
- **Rate limiting para impedir abusos.** É essencial ter controles granulares que possam mitigar ataques DDoS de alta precisão na Camada 7, impedir abusos da API para garantir a disponibilidade, proteger informações sensíveis do cliente contra ataques de login por força bruta e proteger servidores de origem contra a exaustão de recursos, tudo isso evitando custos imprevisíveis por conta de picos de tráfego.

- **WAFs que são atualizados de modo rápido e automático.** Os invasores domésticos na China mostraram ser capazes de tirar proveito de novas vulnerabilidades de aplicativos web muito rapidamente. As organizações podem querer criar regras de WAF próprias, mas não devem confiar apenas em sua inteligência contra ameaças e na capacidade de fazer atualizações. Elas precisam considerar firewalls de aplicativos web que sejam atualizados automaticamente com base em um amplo conjunto de ameaças observadas. E quando a organização quiser fazer suas próprias atualizações de regras, ela deve se sentir confiante de que essas mudanças se propagarão o mais rápido possível.
- **Opções de criptografia personalizáveis.** Para proteger os dados em trânsito na ausência de TLS 1.3 e ESNI, as organizações devem considerar serviços de segurança que oferecem uma ampla variedade de métodos de criptografia personalizáveis.

Os serviços de segurança da Cloudflare, que estão disponíveis como parte da nossa China Network, oferecem mitigação de DDoS sem latência e um WAF de atualização rápida que se baseia na inteligência contra ameaças global. Saiba mais na próxima seção deste documento.

Como a Cloudflare ajuda sites globais que atuam na China

A Cloudflare opera uma rede de data centers presente em 200 cidades de 100 países. Na China, desde março de 2022, há 45 data centers em 38 cidades. Cada um desses data centers pode executar uma ampla variedade de serviços de segurança, performance e confiabilidade, incluindo entrega de conteúdo, resolução de DNS, mitigação de DDoS, imposição de WAF, execução de código sem servidor e muito mais. Como esses serviços são oferecidos em todos os data centers, eles funcionam muito perto dos usuários finais, ajudando a reduzir a latência e dando à nossa rede uma visão detalhada e atualizada das ameaças e condições de rede mais recentes. Além disso, as organizações podem gerenciar todos esses serviços em um único painel.

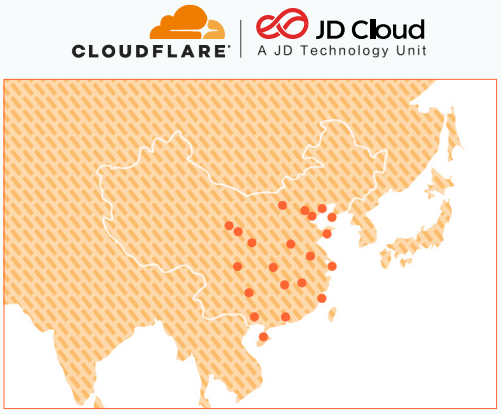
A Cloudflare ajuda organizações a oferecer uma experiência de internet segura, rápida e confiável a visitantes na China desde 2015. A fim de melhorar ainda mais esses serviços, lançamos recentemente uma parceria com a JD Cloud, a unidade de negócios em nuvem e tecnologia inteligente da gigante chinesa da internet JD.com.

Veja como essa rede ajudará as organizações a superar os desafios abordados na seção anterior.

Como a Cloudflare ajuda a superar a latência

A Rede da Cloudflare e da JD Cloud na China oferece:

- **Argo Smart Routing:** transmitir dados do cliente para a origem e depois enviá-lo de volta pode criar latência. Com o armazenamento em cache, o conteúdo estático evita a congestão da rede, mas o conteúdo dinâmico precisa de disponibilidade, confiabilidade e performance na internet. Isso pode levar a tempos de carregamento lentos, exceder o tempo limite, desconexões e uma experiência do usuário degradada. O **Argo Smart Routing** tem o recurso único de **detectar a congestão em tempo real** e **rotear o tráfego da web** para os **caminhos de rede mais rápidos e confiáveis**. Solicitações de clientes da Cloudflare e dos usuários deles feitas à Rede da Cloudflare nos ajudam a entender o a performance de diferentes partes da internet em um determinado momento. O Argo Smart Routing utiliza dados de tempo coletados pela Cloudflare para **rotear dinamicamente o tráfego para os caminhos mais rápidos até a origem**, aumentando a performance. Em média, o Argo melhora o a performance de ativos da web em aproximadamente 30%. Em consequência, isso aumenta as vendas e a retenção.
- **Armazenamento em cache e veiculação de conteúdo estático de muitos data centers na China**, oferecendo menor latência e tempos de carregamento de página mais rápidos, independentemente do local do usuário final. Nossa Rede está estreitamente interconectada com todos os provedores chineses para reduzir o número de saltos de rede realizados pelo tráfego.



Data centers na China Continental

- **Resolução de DNS opcional na China**, que resulta novamente em tempos de resposta mais rápidos.
- A capacidade de **usar o Protocolo de internet versão 6** (IPv6), que permite roteamento e processamento de pacotes eficientes.
- A capacidade de **minimizar o código do site** por meio do nosso recurso de Minificação Automática, que pode ser facilmente ativado marcando uma caixa no Painel de controle da Cloudflare.
- **Computação sem servidor** por meio do serviço Cloudflare Workers, que está presente em todos os data centers da nossa China network e permite responder a determinadas solicitações de maneiras personalizáveis, aumentar os aplicativos existentes e até mesmo criar outros totalmente novos sem configurar ou manter a infraestrutura.

Como a Cloudflare ajuda a lidar com ataques cibernéticos domésticos persistentes

Os serviços de segurança integrados à nossa China network permitem que as organizações:

- **Mitiguem ataques de DDoS.** Cada um de nossos data centers na China pode mitigar ataques, dando à rede uma imensa capacidade de absorver os maiores ataques sem perder solicitações legítimas — e sem depender de data centers da Cloudflare em outro lugar do mundo. Como a inspeção de tráfego acontece perto dos usuários finais, as solicitações deles não passam pelo processo demorado de backhaul para um "centro de depuração" potencialmente distante. E, devido aos desafios de rede na China, a Cloudflare oferece recursos exclusivos e automatizados de engenharia de tráfego que permitem redirecionar automaticamente o tráfego de ataque. Todos esses recursos evitam a diminuição de performance do tráfego legítimo dentro e fora da China.
- **Protejam vulnerabilidades de aplicativos web** com o Cloudflare WAF. Além de impedir vetores de ataque conhecidos com os conjuntos de regras gerenciadas (como a implementação de regras do OWASP e regras próprias da Cloudflare), o WAF conta com um fluxo contínuo de inteligência contra ameaças da nossa Rede para impedir automaticamente as ameaças mais recentes. Além disso, as organizações podem criar facilmente regras próprias — e propagá-las para toda a rede em questão de minutos. Com as melhorias realizadas em 2021, é possível implantar o WAF com mais rapidez e escalar sem dificuldades para cobrir ainda mais tráfego. O WAF também tem conjuntos de regras atualizados que promovem um controle melhor, separando o status da regra da ação. Agora, os usuários navegam melhor nas regras com a filtragem avançada, a edição em massa, as tags de regra etc.
- O **Rate Limiting** está integrado às regras personalizadas do WAF e protege contra ataques DDoS, tentativas de login por força bruta, sobrecarga do servidor de origem e outros tipos de abusos a APIs e aplicativos. É possível configurar limiares, definir o tráfego, personalizar respostas e extrair informações valiosas valiosos de URLs específicas de sites, aplicativos e endpoints da API.
- **Criptografem dados usando TLS 1.2** e gerenciem facilmente as próprias certificações no Painel de controle da Cloudflare.

SAIBA MAIS

O serviço China network está disponível para todos os clientes Enterprise da Cloudflare. Vale lembrar que todas as leis e regulamentações chinesas são cumpridas em relação à exigência de uma licença ICP para integração na China network.

À medida que a economia da internet da China continua a crescer, novos desafios de segurança e performance surgirão inevitavelmente. Os planos da Cloudflare para o crescimento contínuo na China posicionam as empresas em nossa Rede para responder rapidamente a esses desafios e continuar elevando o padrão para experiências do usuário integradas.

Fale com a Cloudflare para começar a otimizar sua presença na web da China agora mesmo!

Para saber mais sobre a China Network da Cloudflare, visite https://www.cloudflare.com/pt-br/china-network/ ou fale com seu representante Cloudflare.