CLOUDFLARE®

Não fique para trás

Como aumentar o desempenho e a segurança do seu site de comércio eletrônico para consumidores de serviços móveis

1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com

Sumário executivo

O ambiente móvel está prestes a tornar-se o canal mais importante para as estratégias de comércio eletrônico. 25% dos principais varejistas dos Estados Unidos já descobriram como elevar as taxas de conversão no ambiente móvel para conquistar uma parcela acima da proporção do mercado acessível, em uma corrida em que os vencedores são absolutos. Eles conseguem uma melhor retenção de usuários e atrair visualizações de produtos oferecendo sites e aplicativos móveis velozes e disponíveis. A Cloudflare pode ajudar a conquistar essas requisitos cruciais, oferecendo:

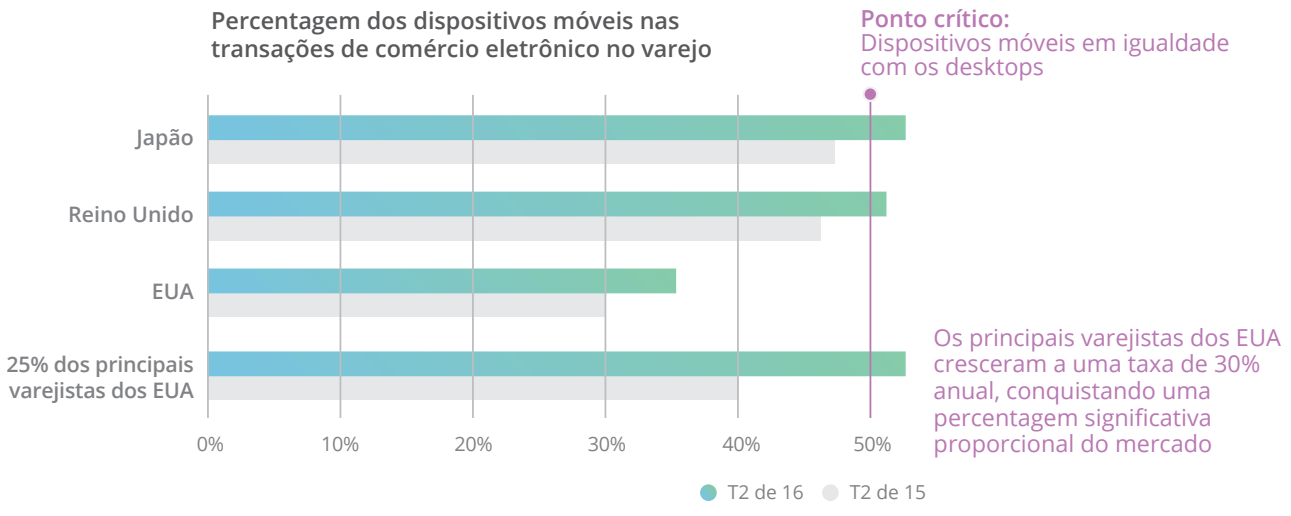
- Uma das mais velozes redes de distribuição de conteúdo, baseada em roteamento Anycast e capaz de armazenar em cache fisicamente próximo dos usuários para reduzir a latência.
- Preço fixo previsível
- Imagens móveis e otimização de código, assim como compatibilidade com IPv6, para reduzir a latência em dispositivos móveis
- Proteção contra ataques de DDoS de camadas 3 e 4 e contra vulnerabilidades de aplicativos de camada 7 para aumentar o tempo de disponibilidade
- Criptografia correta com alto desempenho

A implantação do Cloudflare para ter acesso a esses recursos é um grande passo para fornecedores de comércio eletrônico proativos manterem seus sites velozes e seguros durante todo o ano.

O comércio móvel encontra-se em um momento decisivo

O comércio eletrônico é emocionante: com um crescimento anual de 14,6% e responsável pelo expressivo aumento de 36,2% nas vendas no varejo nos Estados Unidos em 2015, ultrapassou de longe o crescimento observado nas lojas físicas. O comércio móvel encontra-se em um momento decisivo: pela primeira vez na história, no segundo semestre de 2016 no Japão e no Reino Unido, a fatia de mercado das transações no comércio eletrônico varejista foi de 50%, maior do que as transações realizadas em desktops. Nos Estados Unidos, a fatia de mercado do ambiente móvel nas transações de comércio eletrônico está crescendo rapidamente, a 17% anuais. Muito embora a fatia móvel das transações de comércio eletrônico ainda seja menor, com 35%, ela deverá aumentar nos principais países.

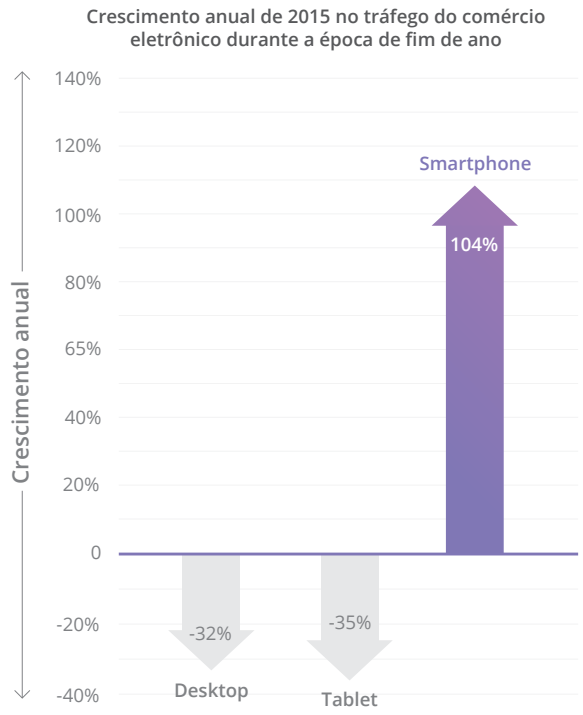
Os 25% principais varejistas dos Estados Unidos já estão capitalizando sobre essa tendência, oferecendo os melhores sites e aplicativos móveis. Eles conseguem melhor retenção de usuários e atraem mais visualizações de produtos, elevando as taxas de conversão em até 90% em relação ao varejista emergente médio. Consequentemente, estão conquistando uma fatia do mercado móvel acima da proporção, com 52% das vendas de comércio eletrônico geradas no ambiente móvel, crescendo a uma taxa impressionante de 30% ao ano.

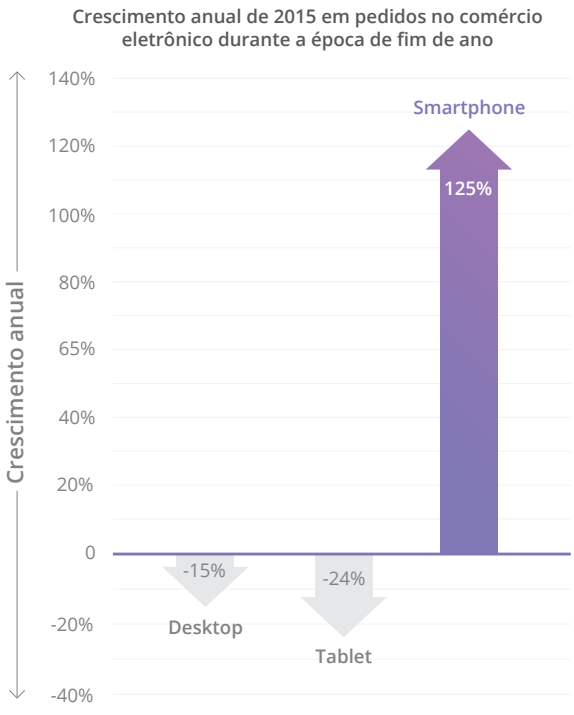


Não há dúvidas de que o comércio online transformou-se em um canal importante de vendas e marketing. Os varejistas que oferecerem a melhor experiência móvel serão os vencedores e continuarão conquistando uma parcela cada vez mais dominante do mercado disponível.

O ambiente móvel tem importância crítica para o período de compras de fim de ano

As compras de fim de ano online (Cyber 5) bateram recordes em 2015, com o Cyber Monday levando o título de dia de maiores gastos online na história dos Estados Unidos. Os smartphones tiveram um papel extremamente importante, respondendo por 49% do tráfego e 27% dos pedidos. O tráfego e os pedidos em smartphones apresentaram taxas de crescimento impressionantes, em detrimento do tráfego e dos pedidos em desktops e tablets, que reduziram proporcionalmente.



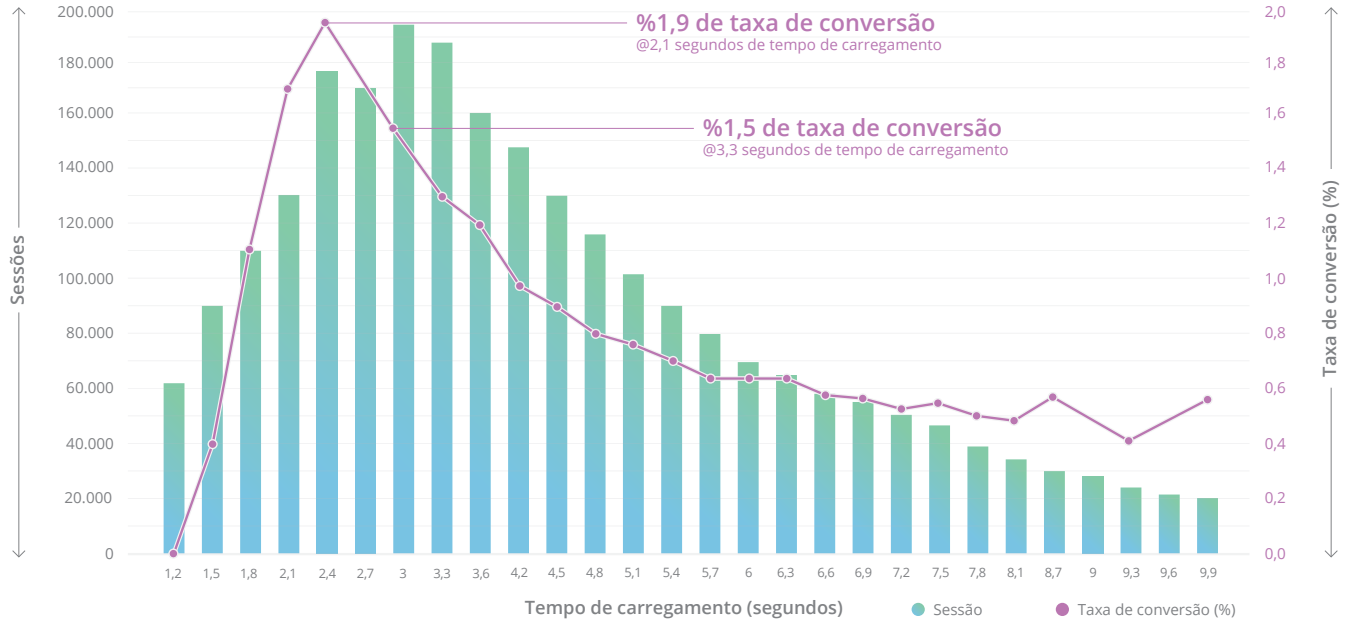


O período de vendas Cyber 5 de 2015 prova novamente que os varejistas com a melhor experiência móvel limpam a banca. Por exemplo, a Amazon teve crescimento de 24,1% no período Cyber 5 de 2015 em relação ao de 2014. Na próxima temporada, os varejistas com presença offline e online provavelmente terão mais tráfego online do que nas lojas, tornando fundamental a experiência de compras móveis para o crescimento.

O impacto da latência e da disponibilidade nas taxas de conversão

O que separa os líderes dos demais? Os líderes do comércio eletrônico oferecem os melhores sites e aplicativos móveis para aumentar suas taxas de conversão. As taxas de conversão do ambiente móvel ainda são baixas e estão diretamente ligadas ao desempenho e à disponibilidade do site ou aplicativo. Por exemplo, a taxa de conversão de um grande varejista online alcançou seu máximo em 1,9% com um tempo médio de carregamento de página de 2,4 segundos. Um tempo médio de carregamento de página somente um segundo maior, de 3,3 segundos, levou a uma queda de 27% na taxa de conversão.

Taxas de conversão de dispositivos móveis por tempos de carregamento da página

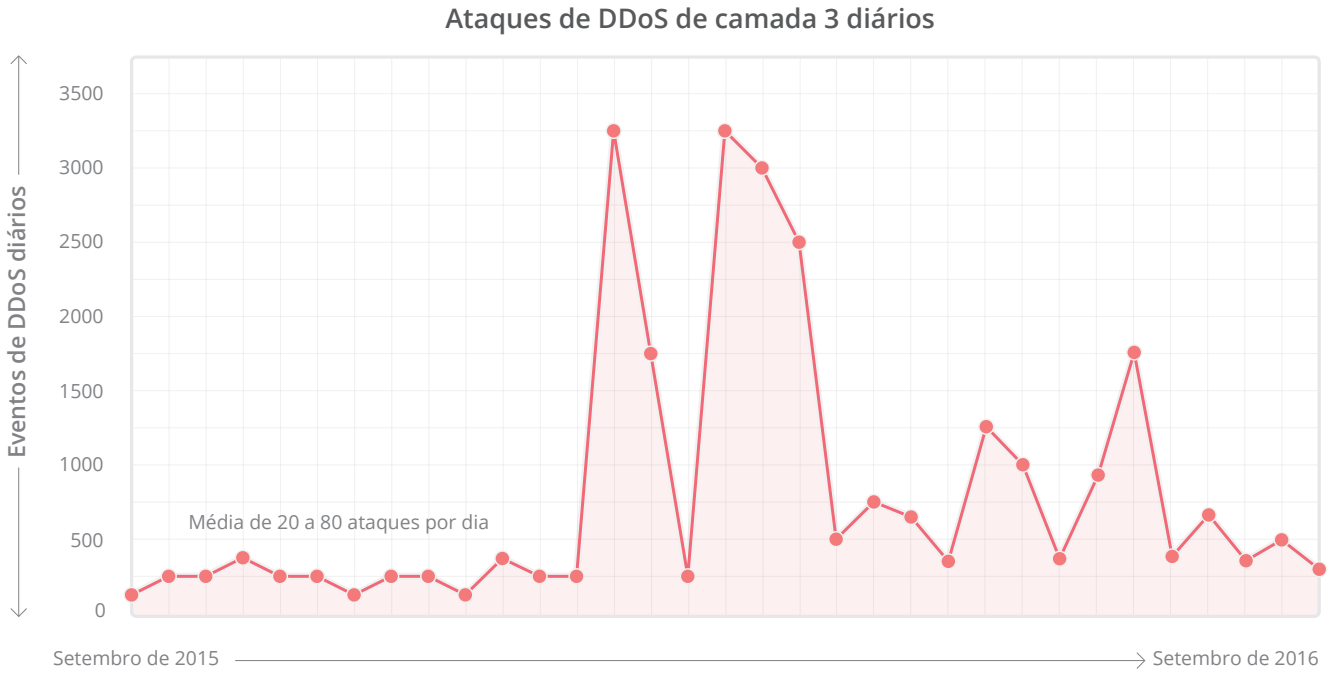


Há muitos exemplos no setor, que ilustram o vínculo entre o desempenho do site e a taxa de conversão.

- A Amazon elevou a receita em 1% para cada 100ms de redução na latência do site
- O Yahoo elevou a o tráfego em 9% para cada 400ms de redução na latência do site
- O Walmart teve um forte declínio nas taxas de conversão quando o tempo médio de carregamento do site aumentou de 1 para 4 segundos.

De uma forma geral, o Google reportou que a latência do site de 100 a 400 milissegundos exerce impacto mensurável no comportamento dos consumidores, e um site que for 250 milissegundos mais lento do que o de um concorrente será visitado com menor frequência.

Além da latência causada pelos próprios sites e aplicativos, os ataques de negação de serviço distribuídos, os ataques de DDoS, podem tornar o site totalmente indisponível. A CloudFlare, que tem próximo de 10% do tráfego de internet mundial fluindo por suas redes, é capaz de filtrar os ataques e medi-los com precisão. No ano passado a CloudFlare registrou aumento no número e na intensidade dos ataques, com até 1.400 eventos diários de DDoS, um tráfego agregado de entrada de 400 GBps e ataques com 200 milhões de pacotes por segundo.



Muitas vezes os ataques não são eventos isolados e normalmente as vítimas são alvejadas diversas vezes em um ano. De acordo com a experiência da CloudFlare, qualquer empresa, sejam organizações de pequeno ou grande portes, podem ser alvejadas. Muito embora muitas jurisdições contam com leis sob as quais os ataque de DDoS são ilegais, há provedores de DDoS-como-serviço oferecendo assinaturas, algumas com valores tão baixos quanto cinco ou dez dólares mensais.

Até mesmo o site da Amazon (US$ 99 bilhões em receitas no varejo em 2015) ficou fora do ar diversas vezes no passado por razões desconhecidas. Por exemplo, em 2013 o Amazon.com ficou fora do ar por um tempo estimado de 15 a 45 minutos, custando à empresa um prejuízo de US$1,8 a US$ 5,3 milhões em vendas não realizadas, com base na média de US$ 117,882 em vendas por minuto. O custo da indisponibilidade para fornecedores de comércio eletrônico pode ser muito mais alto no período de compras de fim de ano. A Amazon divulgou 33% de receitas anuais no quarto trimestre de 2015, devido à sazonalidade do negócio. Outrosefeitos negativosda indisponibilidade do sistema são o impacto na satisfação do cliente, a classificação nos sistema de busca e as relações com os investidores.

Resumindo, é fundamental para os fornecedores de comércio eletrônico que desejam melhorar as taxas de conversão, especialmente durante o período de festas de fim de ano, oferecer sites e aplicativos rápidos, protegidos contra ataques de DDoS, para melhorar o tempo de disponibilidade.

Tecnologias essenciais para sites móveis rápidos e seguros

A Cloudflare pode ajudá-lo a acelerar e proteger seus sites e aplicativos de comércio móvel, sem a adição de hardware ou a instalação de software, ou mesmo sem alterar uma única linha do seu código.

O primeiro passo é usar a rede de distribuição de conteúdo (CDN) da Cloudflare, uma das maiores redes do mundo, responsável por mais de 10 trilhões de solicitações mensais. São quase 10 por cento de todas as solicitações da internet para mais de 2,5 bilhões de pessoas em todo o mundo. A CDN da Cloudflare é constantemente classificada como uma das mais velozes, com tempos médios de resposta de 34 ms (nos EUA), de acordo com a Cedexis. Alguns dos seus principais recursos são:

Roteamento baseado em Anycast

Embora a CDN da Cloudflare funcione com um método de roteamento conhecido como Anycast, a maior parte da internet atual ainda funciona com um mecanismo chamado unicast. No unicast, todos os nós da rede recebem um endereço IP, que é exclusivo do nó. Os roteadores mantêm um mapa dos endereços IP do mundo, para manter informações sobre as rotas mais curtas entre os diversos saltos para alcançar o destino final. Entretanto, o destino final pode estar em algum ponto do outro lado do continente ou em algum outro lugar do outro lado do mundo, exigindo saltos adicionais, cada um adicionando mais latência. No Anycast, o método de roteamento usado pela Cloudflare, diversas máquinas da rede CDN têm o mesmo endereço IP remoto, permitido que os roteadores enviem solicitações diretamente ao servidor mais próximo fisicamente para reduzir a latência.

Cache de conteúdo

A rede Anycast da Cloudflare funciona em conjunto com o cache de conteúdo. Uma vez que o Anycast rotear uma solicitação para o servidor fisicamente mais próximo, uma cópia do conteúdo em cache fica disponível para o acesso nesse servidor. O benefício do cache é que os objetos podem ser movidos até mais próximo do visitante que os solicitar para acelerar a entrega e para reduzir a carga no servidor web de origem. A Cloudflare oferece recursos para fazer o cache automático de conteúdo estático e, com o Railgun, a Cloudflare oferece um mecanismo para fazer o cache de conteúdo dinâmico.

A Cloudflare analisa o tráfego que volta aos servidores na CDN para localizar as partes estáticas do site de origem. Em seguida o conteúdo estático é armazenado em cache na CDN por um curto período de tempo. Normalmente 66% do conteúdo da web pode ser armazenado em cache (por meio de “cache automático do conteúdo estático”) e os 34% restantes não podem ser armazenados e devem ser obtidos do servidor de origem. O Railgun foi projetado para agilizar a entrega de conteúdo que não pode ser armazenado em cache, para que basicamente toda a web possa ser armazenada. Funciona reconhecendo que as páginas da web que não podem ser armazenadas em cache não se alteram com muita rapidez e que as diferenças muito pequenas nas alterações entre as versões das páginas da web podem ser identificadas pelos servidores da CDN da Cloudflare. A Cloudflare então comprime as alterações com taxas de compressão de até 99,6% e as envia pelo link, obtendo melhorias de desempenho de até 700%. O Railgun exige a instalação de um componente de software no lado do servidor de origem.

"Como os custos de largura de banda continuam subindo, ter uma CDN como a Cloudflare servindo imagens no limite aos usuários, é econômico e reduz a latência de nossos clientes móveis"

Chris Smith, diretor de comércio eletrônico, Big 5 Sporting Goods

Preço fixo

Para fazer parte da Internet, a Cloudflare compra largura de banda, conhecida como trânsito, de diversos provedores. A Cloudflare compra trânsito no atacado com base na capacidade usada em qualquer mês, pagando pela máxima utilização por um período. Embora a taxa paga pela Cloudflare varie dramaticamente nas diversas regiões do mundo, para manter a simplicidade dos preços a Cloudflare cobra dos clientes uma taxa fixa, independente de onde o tráfego será entregue em qualquer lugar do mundo. Ao contrário de alguns serviços de nuvem, que cobram por bits transmitidos pela rede, a Cloudflare permite que as contas mensais sejam previsíveis. A Cloudflare continua trabalhando para reduzir o preço do trânsito e aumentando o peering, para oferecer o melhor serviço possível pelo menos preço possível.

Otimização de imagem e código

Com Polish, Mirage e Auto-Minify, a Cloudflare oferece uma solução em três partes para reduzir a latência. Esses recursos são especialmente importantes para dispositivos móveis, que têm larguras de banda limitadas.

O Polish remove os metadados e comprime as imagens para reduzir o tamanho. O Polish também pode ser executado no modo sem perdas (Lossless), o que remove o excesso desnecessário do cabeçalho e dos metadados da imagem, sem remover qualquer informação da imagem. A redução média do tamanho é de 21%. O Polish pode também ser executado no modo com perdas (Lossy) que, além do Lossless, aplica um algoritmo de compressão às imagens adequadas. As imagens serão exibidas exatamente da mesma maneira que teriam sido exibidas antes, sem qualquer diferença visual perceptível, mas os tamanhos dos arquivos são reduzidos em média em 48%. As imagens respondem por mais de 50% dos dados que formam um site típico.

O Mirage gerencia a maneira como as imagens são carregadas nos dispositivos móveis. Ele cria rapidamente a apresentação de uma página utilizável com que os usuários podem interagir, enquanto preenche o restante da página sem prejudicar a experiência do usuário.

- O Mirage utiliza o carregamento lento para priorizar o carregamento das imagens que se encontram no visor, ou seja, as imagens que são de fato exibidas pelo navegador. Em seguida carrega as demais imagens da página, que não são exibidas pelo navegador, à medida que forem necessárias ou se houver recursos de rede livres disponíveis.
- Os dispositivos móveis exigem imagens menores, devido ao tamanho das telas. O Mirage redimensiona a imagem no servidor, normalmente a 1% da resolução total da imagem, e envia primeiro a imagem com o tamanho reduzido. Depois que a página for apresentada com as imagens reduzidas, serão substituídas pelas versões com resolução completa. As imagens são apresentadas inicialmente com baixa qualidade e, em seguida, com nitidez total.
- Em vez de iniciar uma nova solicitação para cada imagem, o Mirage envia as imagens por stream por meio da rede do Cloudflare com uma única solicitação. Isso significa que uma única página com centenas de imagens pode começar a ser exibida no navegador com apenas duas solicitações. Mesmo os usuários que se encontrarem em conexões móveis lentas poderão começar a interagir com a página imediatamente, em vez de ter que aguardar pelo carregamento de todas as imagens com resolução total.

O Auto Minify remove instantaneamente todos os caracteres desnecessários, ou seja, os "espaços em branco", de arquivos HTML, JavaScript e CSS, economizando 20% do tamanho do arquivo, sem alterar o funcionamento. A implementação do Auto Minify pela Cloudflare é facilmente 100 vezes mais rápida do que o método mais próximo.

Compatibilidade com IPv6

Medidas de monitoramento real de usuários do Facebook e do Linkedin mostraram que os tempos de carregamento de páginas móveis por IPv6 são bem mais do que 10% mais rápidos do que por IPv4 nas quatro principais redes móveis dos Estados Unidos. Embora o lançamento do IPv6 seja uma atividade que exigirá décadas e esteja sofrendo com a percepção de ser lento, cerca de 60% das solicitações do Android e 20% das solicitações do iPhone das quatro principais redes móveis dos Estados Unidos usaram IPv6 em sites de pilha dupla (em 4/5/2016). A Cloudflare não apenas oferece compatibilidade total com IPv6, como também um gateway IPv6-para-IPv4 desde 2012. A Cloudflare torna também "simples como um clique" para os clientes ativarem o serviço. Se o servidor de origem for compatível com IPv6, os visitantes que chegarem com conexão IPv6 serão transportados por meio do protocolo, de ponta a ponta. Se o servidor de origem for compatível somente com IPv4, a Cloudflare aceitará um visitante por IPv6 e fará, sem problemas, a solicitação ao servidor por meio de IPv4. Além disso, se um aplicativo que estiver utilizando no servidor de origem exigir IPv4, a Cloudflare fornece o pseudo IPv4. Sempre que a conexão for estabelecida em IPv6, essa opção adicionará um cabeçalho HTTP às solicitações com um endereço "pseudo" IPv4.

Proteção contra DDoS em camadas 3 e 4 - Resiliência da rede Anycast com plataforma de aprendizado automático

Além de usar rede de distribuição de conteúdo da Cloudflare, o próximo passo será proteger o site ou os aplicativos contra ataques maliciosos para garantir a disponibilidade. A proteção contra ataque de DDoS da Cloudflare, provisionada como um serviço na borda da rede, tem a mesma sofisticação e a mesma dimensão das ameaças e pode ser usada para mitigar os ataque de DDoS de todas as forma e tamanhos. A Cloudflare impediu diversos do maiores ataque de DDoS, inclusive ataques com mais de 400 Gbps.

Normalmente os ataque de DDoS de camadas 3 e 4 são ataques volumétricos, como ataques DDoS, de amplificação, inundação DDoS e inundação DDoS SYN. Embora esses ataques possam sobrecarregar uma rede com base unicast normal, a rede com base em Anycast da Cloudflare aumenta de forma inerente a superfície, espalhando o tráfego do ataque para todas as mais de 100 centrais de dados da Cloudflare e para um conjunto variado interconexões de banda larga com outras redes, para simplesmente absorver o tráfego do ataque. Além disso, a Cloudflare oferece uma plataforma de aprendizado automático, onde o tráfego de rede é analisado em tempo real para identificar solicitações anômalas ou maliciosas. Depois que um novo ataque é identificado, o Cloudflare inicia automaticamente o bloqueio desse tipo de ataque, para o site em questão e toda a comunidade.

Mesmo no que diz respeito ao custo, normalmente os ataques não afetam a Cloudflare, já que ela compra quantidades consideráveis de banda e paga pelo nível mais alto de tráfego de entrada ou saída médio verificado em um mês. Como a Cloudflare funciona como um proxy de cache, em circunstâncias normais o tráfego de saída excede o de entrada, geralmente em cerca de quatro ou cinco vezes. Quando há um ataque, as duas linhas se aproximam, mas raramente um ataque é suficientemente grande para aumentar os custos com banda da Cloudflare. A Cloudflare repassa esse benefício a seus clientes, e os clientes não são cobrados por um aumento no tráfego de rede causado por um ataque de DDoS.

À medida que a Cloudflare continuar ampliando sua rede e sua comunidade, será ainda mais difícil lançar um ataque de DDoS eficaz contra qualquer um dos usuários da Cloudflare.

Proteção contra DDoS de camada 7: Rate Limiter com banco de dados de reputação de IPs

Assim como os ataques volumétricos de camadas 3 e 4, os ataques de DDoS usam um alto volume de solicitações para impedir que os usuários reais acessem o site. Nos ataques de DDoS de camada 7, um único endereço IP realiza muitas solicitações, semelhantes ao padrão de tráfego normal e não malicioso, e assim são de difícil proteção.

O Protetor de tráfego da Cloudflare, disponível atualmente por meio de um programa de acesso inicial, acompanha o número de solicitações enviadas a um site de cada endereço IP, e identifica os sites que estiverem fazendo um número excessivo de solicitações por minuto. Depois que um endereço IP suspeito for identificado, o tráfego desse endereço IP será apresentado com uma página intersticial por cerca de cinco segundos para realizar uma série de verificações matemáticas. Se a solicitação não passar nessa verificação, o Protetor de tráfego reduzirá a reputação desse IP e será apresentado um CAPTCHA ao tráfego desse endereço em todas as tentativas de acesso.

Quando a Cloudflare identificar um endereço IP que parecer estar fazendo solicitações maliciosas, ele será armazenado no banco de dados de reputação de IPs da Cloudflare. Com base em uma pontuação de ameaça, uma solicitação poderá passar ou receberá um CAPTCHA. Se o CAPTCHA falhar e o endereço IP for identificado como malicioso, a solicitação será bloqueada na borda da Cloudflare para toda a rede, beneficiando toda a comunidade da Cloudflare.

Ataques de vulnerabilidade de aplicativo não DDoS em camada 7: firewall de aplicativo Web

Os ataques de camada de aplicativo de camada 7 são os tipos de ataques mais complexos e sofisticados. Imitando a utilização normal de um aplicativo, eles conseguem passar pela maioria dos equipamentos de mitigação de DDoS e serviços de proteção de vulnerabilidades. Os tipos comuns de ataques incluem injeção de SQL e scripts entre sites (XSS), que podem permitir que os agressores acessem e alterem dados dos clientes e quaisquer tipos de dados do sistema.

A Cloudflare cuida dessas ameaças por meio do seu firewall de aplicativo Web (WAF). O WAF implementa o conjunto básico de regras OWASP, que são as regras implementadas e prontas para uso da Cloudflare, além de regras personalizadas criadas pela comunidade e pelos clientes. Uma nova regra liberada pela Cloudflare será propagada a todos os nós de servidores da Cloudflare dentro de 30 segundos, e o próprio WAF adicionará menos de 1ms de latência por solicitação, oferecendo segurança sem qualquer ônus no desempenho. Dessa forma, a Cloudflare conseguiu proteger seus clientes contra as principais vulnerabilidades aos ataques de Dia Zero, inclusive a vulnerabilidade Shellshock ou o bug Heartbleed.

"Tratamos o impacto dos ataques de DDoS com muita seriedade. Mesmo nos casos em que nosso domínio enfrentou um ataque de DDoS, a Cloudflare conseguiu proteger nosso domínio rapidamente, oferecendo uma experiência tranquila para nossos clientes. O maior benefício oferecido pela Cloudflare é a tranquilidade de que há alguém monitorando a rede e que há uma maneira de mitigar qualquer ataque".

Chris Smith, diretor de comércio eletrônico, Big 5 Sporting Goods

TLS 1.3 e HTTP/2 com push de servidor

Criptografia é essencial para proporcionar uma experiência de compras confiável, mas os mais recentes aprimoramentos no SSL podem ser usados para aumentar o desempenho. O Transport Layer Security 1.3 (TLS) não somente remove as características inseguras das versões de TLS anteriores, mas também reduz a latência, cortando pela metade o percurso de ida e volta do protocolo. A Cloudflare foi a primeira a implementar o TLS 1.3, e contribuiu consideravelmente com o padrão. A Cloudflare também foi a primeira a implementar o HTTP/2, que funciona somente com TLS. O HTTP/2 melhora o desempenho, especialmente a latência, conforme constatado pelo usuário final no uso de um navegador. O HTTP/2 funciona em conjunto com o Server Push, em que um servidor pode enviar recursos que o cliente ainda não solicitou, para acelerar ainda mais o desempenho percebido. O TLS 1.3 e o HTTP/2 com push de servidor são apenas dois exemplos do trabalho da Cloudflare para integrar constantemente tecnologias emergentes à sua rede.

Conclusões

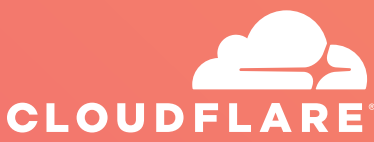
Inscreva-se na Cloudflare para melhorar o desempenho do seu site e dos seus aplicativos móveis, ao mesmo tempo protegendo-os dos ataque de DDoS e das vulnerabilidades dos aplicativos. A configuração é fácil e normalmente demora menos de cinco minutos para entrar em funcionamento. Consulte os planos, desde os gratuitos até os corporativos, em www.cloudflare.com.

Fale conosco para saber mais sobre a Cloudflare.

www.cloudflare.com

enterprise@cloudflare.com

1 888 99 FLARE



1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com