Proteção contra DDoS com Cloudflare

A evolução dos ataques modernos de DDoS

2016

1 Tbps

Ataque de botnet de IoT de camada 7

O maior ataque de camada 7 da história usou um botnet de IoT Mirai. Foi um ataque volumétrico que usou recursos de servidor.

2014

400 Gbps

Ataque de amplificação de NTP

O responsável pelo ataque usou 4.529 servidores para amplificar o ataque do servidor de origem, que tinha apenas 87 Mbps

2013

120 Gbps

Ataque DDoS de camada 3/4

O ataque de Spamhaus foi considerado um dos maiores de todos e chamado de "o ataque que quase quebrou a Internet".

Os ataques distribuídos de negação de serviço (DDoS, Distributed Denial of Service) têm aumentado e evoluíram para desafios de segurança complexos e avassaladores para as empresas. Embora não sejam um fenômeno recente, os métodos e recursos disponíveis para conduzi-los e mascará-los evoluíram dramaticamente. A formação do botnet Mirai foi um marco na evolução dos ataques DDoS. Esse botnet era composto por mais de 300 mil dispositivos de IoT hackeados que foram usados para gerar o maior ataque DDoS conhecido, com pico de tráfego que excedeu 1 Tbps em throughput.

Em geral, os ataques DDoS não são eventos isolados e suas vítimas são alvejadas várias vezes ao ano. De acordo com a experiência da Cloudflare, qualquer empresa, seja grande ou pequena, pode ser um alvo. Embora várias jurisdições contem com leis que proíbem os ataques DDoS, existem provedores de DDoS como serviço que oferecem assinaturas, algumas com preços iniciais tão baixos quanto US$ 5 a US$ 10/mês.

A perda de receita é apenas uma das várias ameaças que esse tipo de ataque pode trazer para seu site ou empresa. Até mesmo o site da Amazon (US$ 99 bilhões em vendas no varejo em 2015) já saiu do ar várias vezes por motivos desconhecidos. Em 2013, por exemplo, o Amazon.com saiu do ar durante aproximadamente 15 a 45 minutos, o que custou US$ 1,8 a US$ 5,3 milhões em vendas perdidas, considerando a média de venda de US$ 117.882 por minuto da empresa. Além disso, fatores como a inacessibilidade do site causam perdas menos quantificáveis, como a degradação da marca e a piora da satisfação do cliente.

Solução dimensionável e precisa para DDoS

Uma rede Anycast™ global de 10 Tbps da Cloudflare é dez vezes maior do que o maior ataque DDoS da história, permitindo que todos os ativos da Internet que estejam na rede da Cloudflare suportem os enormes ataques DDoS de hoje. A proteção contra DDoS da Cloudflare para as camadas 3, 4 e 7 está disponível como serviço nos limites da rede, correspondendo à escala das ameaças modernas, e pode ser usada para mitigar ataques DDoS de todos os tipos e portes. A limitação de taxa complementa a proteção contra DDoS da Cloudflare, permitindo a mitigação precisa dos ataques mais sofisticados à camada de aplicativos.

PROTEÇÃO CONTRA ATAQUES DDOS NAS CAMADAS 3 E 4

Os ataques DDoS nas camadas 3 e 4 geralmente são volumétricos, como os ataques de amplificação de DDoS, flood de DDoS e flood de SYN DDOS. Embora esses ataques possam sobrecarregar as redes comuns baseadas em unicast, a rede da Cloudflare, baseada em Anycast, aumenta inerentemente a superfície ao espalhar o tráfego do ataque pelos mais de 102 centros de dados da Cloudflare e por um conjunto diverso de interconexões de grande largura de banda, absorvendo esse tráfego de ataque.

Recursos de proteção contra DDoS

- Proteção contra DDoS de camadas 3, 4 e 7
- Proteção contra ataques de DNS
- Bloqueio refinado de ameaças com limitação de taxa
- Segurança preditiva com banco de dados de reputação de IP

"Sabendo que não temos de nos preocupar com os ataques DDoS contra a API e os servidores de gateway, temos tranquilidade para manter o foco na melhoria de nosso produto."

– Jake Heinz, engenheiro de software da Discord

Rede da Cloudflare

- Rede Anycast™ global com mais de 102 centros de dados
- Throughput de 10 Tbps para absorver ataques volumétricos
- 6 milhões de propriedades da Internet
- Preço fixo por largura de banda

"Usamos Cloudflare porque os recursos de segurança são excelentes, o CDN tem alto desempenho e é muito conveniente que essas soluções sejam vendidas em conjunto. Facilita o gerenciamento de tudo e permite que nos concentremos em nossas atividades principais."

– Amanda Kleha, gerente geral, unidade de negócios da Zendesk Online

PROTEÇÃO CONTRA VULNERABILIDADES DE APLICATIVOS NA CAMADA 7

Entre os tipos comuns de ataques de camada 7, estão a injeção de SQL e o script cross-site (XSS, Cross-Site Scripting), que podem permitir que o atacante acesse e manipule dados de clientes ou outros tipos de dados de aplicativos. A Cloudflare enfrenta essas ameaças com o firewall de aplicativo Web (WAF, Web Application Firewall). O WAF bloqueia automaticamente as ameaças encontradas no conjunto de dez regras principais do OWASP, nos conjuntos de regras da Cloudflare e em regras personalizadas criadas pela comunidade ou pelos clientes. A Cloudflare tem conseguido proteger seus clientes contra as maiores vulnerabilidades de dia zero, como a vulnerabilidade Shellshock e o Heartbleed Bug.

LIMITAÇÃO DE TAXA

Ative a limitação de taxa da Cloudflare para um controle refinado do tráfego que complementa os serviços de proteção contra DDoS e WAF da Cloudflare. A limitação de taxa protege contra ataques de negação de serviço, tentativas de roubo de senha por força bruta e outros tipos de comportamentos impróprios direcionados à camada do aplicativo. Configure limites de solicitação, defina respostas personalizadas como ações de mitigação (desafios ou CAPTCHAS) ou códigos de resposta e reúna informações analíticas em pontos de extremidade de seu site, aplicativo ou API.

Segurança preditiva

A Cloudflare oferece uma plataforma de aprendizagem automática em que o tráfego de rede é analisado em tempo real para identificar solicitações anômalas ou maliciosas. Assim que um novo ataque é identificado, a Cloudflare começa automaticamente a bloquear esse tipo de ataque no site em questão e na comunidade como um todo. Conforme a rede e a comunidade da Cloudflare crescem, fica cada vez mais difícil lançar um ataque DDoS eficaz contra qualquer usuário da Cloudflare.

Preço fixo por largura de banda

A Cloudflare proporciona proteção contra DDoS ilimitada de nível empresarial a uma mensalidade fixa. A Cloudflare acredita que os clientes não devem ser penalizados pelo aumento no tráfego da rede associado aos ataques DDoS. Com a proteção contra DDoS da Cloudflare, o cliente pode ficar tranquilo, pois seu site permanecerá on-line e os gastos mensais serão fixos.

Inscreva-se na Cloudflare

Inscreva-se na Cloudflare e ative a limitação de taxa para proteger seu site, aplicativo ou API dos ataques DDoS, ao mesmo tempo em que reduz a latência e usa as últimas tecnologias da Web. A configuração é fácil e costuma levar menos de cinco minutos para começar a funcionar. Confira os planos, que vão desde Grátis até Enterprise, em www.cloudflare.com.