Soluções ANTI DDoS existentes no mercado

Autor: Graciela Martínez
Coordenação e revisão: Área de Comunicações
Edição: Área de Comunicações
Área: Área de Tecnologia

Setembro 2024

lacnic
www.lacnic.net

Existem diversas soluções anti-DDoS oferecidas por provedores e empresas no mercado. A seguir, listamos uma série dessas ferramentas disponíveis.

Soluções comerciais

A escolha da melhor solução para cada organização depende de vários fatores, como o orçamento, nível de proteção necessário e infraestrutura existente.

Cloudflare [1]:

Descrição: Cloudflare é uma das soluções mais populares para a mitigação de DDoS. Oferece proteção no nível da rede e aplicativos, com uma infraestrutura global que dispersa o tráfego malicioso.

Características: Proteção DDoS, CDN (Content Delivery Network), WAF (Web Application Firewall) e DNS seguro.

Vantagens: Fácil de implementar, escalabilidade global, análise em tempo real, e rentável para sites de todos os tamanhos.

Akamai:

Descrição: Esta empresa é conhecida por sua rede de distribuição de conteúdo, embora também ofereça recursos robustos de mitigação de DDoS por meio de seu serviço Kona Site Defender.

Características: Proteção em nível de rede e aplicativo, distribuição de tráfego por meio de uma rede global, e ferramentas avançadas de análise e monitoramento.

Vantagens: Ampla rede de distribuição, suporte para grandes volumes de tráfego e alta confiabilidade.

https://www.akamai.com/

Amazon Web Services (AWS) Shield:

Descrição: AWS Shield é uma solução de mitigação de DDoS integrada à infraestrutura de AWS. Disponível em dois níveis: Standard e Advanced.

Características: Proteção contra ataques em nível de rede e aplicativo, integração com outros serviços de AWS e recursos avançados de monitoramento e resposta.

Vantagens: Integração nativa com AWS, proteção automática e escalabilidade, opções de relatórios detalhados e suporte adicional com Shield Advanced.

https://aws.amazon.com/es/shield/

Google Cloud Armor:

Descrição: O Google Cloud Armor fornece proteção DDoS para aplicativos hospedados no Google Cloud, usando a infraestrutura global do Google.

Características: Políticas de segurança baseadas em regras, mitigação de ataques em nível de rede e aplicativos, e proteção contra ataques volumétricos e de aplicativos.

Vantagens: Integração nativa com Google Cloud, fácil de configurar e gerenciar, e escalabilidade global.

https://cloud.google.com/armor/docs?hl=es-419

Imperva Incapsula:

Descrição: Imperva Incapsula oferece proteção DDoS para aplicativos web e serviços baseados na nuvem.

Características: Mitigação de DDoS em nível de rede e aplicativos, WAF, proteção contra bots, e recursos de monitoramento e análise em tempo real.

Vantagens: Proteção abrangente contra vários tipos de ataques, fácil implementação, e opções avançadas de configuração e personalização. https://www.imperva.com/

Arbor Networks (NETSCOUT):

Descrição: Arbor Networks é uma solução de segurança que oferece proteção contra os ataques DDoS, usada tanto por provedores de serviços quanto por empresas.

Características: Detecção e mitigação de ataques em tempo real, inteligência baseada na rede global, e análises detalhadas.

Vantagens: Ampla experiência e reputação em mitigação de DDoS, suporte para grandes infraestruturas e ferramentas de análise avançadas.

https://www.netscout.com/solutions/service-provider-ddos-protection

F5 Networks:

Descrição: A F5 Networks oferece soluções de mitigação de DDoS que protegem aplicativos e redes por meio de seu sistema BIG-IP.

Características: Mitigação de DDoS em nível de rede e aplicativos, WAF, balanceamento de carga, e ferramentas de monitoramento e análise.

Vantagens: Abordagem híbrida de hardware e software, alta confiabilidade e capacidade de lidar com grandes volumes de tráfego. https://www.f5.com/es_es

As ferramentas mencionadas são amplamente usadas devido à sua eficácia e capacidade de lidar com grandes volumes de tráfego, bem como à sua facilidade de integração e uso.

As organizações podem consultar fornecedores de soluções de segurança, bem como os seus ISP, que muitas vezes oferecem serviços de mitigação de DDOS como um valor agregado ao seu serviço de conectividade.

Soluções de código aberto

Existem também ferramentas *open source* (de código aberto) com o mesmo objetivo: mitigação de ataques de DDoS. Entre elas, vale destacar:

Haproxyr:

Descrição: HAProxy é um proxy inverso gratuito, muito rápido e confiável que oferece alta disponibilidade, balanceamento de carga e proxy para aplicativos baseados em TCP e HTTP.

Características: É um balanceador de carga e proxy que pode ajudar a distribuir o tráfego de forma equitativa entre vários servidores.

Vantagens: Pode ser útil para lidar com grandes volumes de tráfego durante um ataque de DDoS.

https://github.com/haproxy

Gatekeeper:

Descrição: Gatekeeper é o primeiro sistema de proteção DDoS de código aberto, usado por operadores de redes institucionais, provedores de serviços e conteúdo, redes empresariais, etc.

Características: Ele foi projetado para escalar para qualquer largura de banda máxima. Sua arquitetura é geograficamente distribuída enquanto a política de rede que descreve todas as decisões que devem ser aplicadas ao tráfego de entrada é centralizada.

Vantagens: Sua capacidade de escalar para qualquer largura de banda faz com que ele possa resistir a ataques DDoS atuais e futuros. Além disso, a sua política centralizada permite que os operadores de rede aproveitem os algoritmos distribuídos que não seriam viáveis com uma latência muito elevada (por exemplo, bases de dados distribuídas) e combater vários ataques DDoS multivectoriais em simultâneo.

https://github.com/AltraMayor/gatekeeper

FastNetMon:

Descrição: FastNetMon: um detector/sensor DDoS de alto desempenho baseado em vários mecanismos de captura de pacotes: NetFlow, IPFIX, sFlow, AF_PACKET.

Características: Detecta hosts na rede que enviam ou recebem grandes volumes de tráfego, pacotes/bytes/fluxos por segundo, e executa uma ação configurável para lidar com esse evento. Estas ações configuráveis incluem notificá-lo, chamar o script ou fazer anúncios BGP.

Vantagens: Tem múltiplas vantagens, tais como: detecção de DoS/DDoS em apenas 1-2 segundos, escalonamento até terabits em um único servidor (sFlow, Netflow, IPFIX) ou até 40G + em modo espelho, permite configurar limiares por sub-redes, possui notificações por e-mail sobre ataques detectados e tem suporte total para o IPv6.

https://github.com/pavel-odintsov/fastnetmon/

Finalmente, devemos mencionar que alguns ISP ou provedores de segurança também oferecem aos seus clientes serviços de depuração de DDoS. Estes consistem em enviar tráfego limpo para a organização após absorver o ataque, porque supostamente possuem inteligência para detectar e descartar a maioria dos tipos de ataques DDoS. Esses serviços devem ser complementados com soluções DNS e BGP para serem eficazes.