Boas práticas e técnicas para mitigar ataques de DDoS

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

Setembro 2024

lacnic
www.lacnic.net

Os ataques DDoS são causados pela exploração de vulnerabilidades nas diferentes camadas da pilha TCP/IP ou pelo abuso da capacidade da rede para lidar com grandes volumes de tráfego. Portanto, é importante implementar uma proteção abrangente na organização. Para isso, compartilhamos com a comunidade diferentes ações que podem complementar uma solução DDoS e proteger servidores e redes.

Esta primeira parte descreve as principais ações que podem ser tomadas pela organização para prevenir ataques de DDOS (diminuir a sua probabilidade de ocorrência e/ou minimizar o seu impacto).

Quanto à configuração da rede e dos serviços para reduzir a probabilidade de ataques DDOS e fortalecer a infraestrutura contra eles, é aconselhável implementar (se possível):

1. **Redundância e distribuição de carga**:

   Usar CDN para proteger sites WEB. As CDN são redes distribuídas de servidores proxy que reduzem a latência uma vez que armazenam conteúdo em cachê e o "aproximam" dos usuários finais. Dessa forma, os ataques de DDoS serão mitigados mais perto da fonte sem afetar o desempenho.

2. **Rate Limiting**:

   Limitar o número de pedidos que um usuário pode fazer em um período específico para evitar abusos.

3. **Filtragem de tráfego**:

   Configurar firewalls e sistemas de detecção de intrusões (IDS) para filtrar o tráfego malicioso com base em padrões e assinaturas conhecidas, bem como usando aprendizado automático.

4. **Anycast Routing**:

   Usar roteamento Anycast para distribuir o tráfego por vários locais, tornando mais difícil para os atacantes concentrarem o ataque em um único ponto.

5. **Capacidade de sobrecarga**:

   Certificar-se de que a infraestrutura possa lidar com uma quantidade significativa de tráfego adicional mediante o uso de servidores e largura de banda adicional.

6. **Proteção em nível de protocolo**:

   Configurar corretamente os protocolos de rede para mitigar vulnerabilidades que levem a ataques de amplificação e, assim, minimizar seu impacto

Em relação ao monitoramento e detecção, é boa prática dispor de:

7. **Sistemas de detecção e resposta precoce**:

   Implementar soluções de monitoramento que detectem padrões de tráfego incomuns e respondam automaticamente a possíveis ataques.

8. **Implementar mecanismos para:**

- Detectar bots maliciosos e bloquear seu tráfego sem interromper o tráfego de usuários legítimos.
- Implementar mecanismos que permitam a diferenciação entre tráfego de ataque e tráfego legítimo.

  Embora diferenciar o tráfego de ataque do tráfego legítimo não seja trivial, existem diferentes ferramentas, projetos e iniciativas que podem ajudar a identificar possíveis padrões de tráfego não desejado. [https://csirt.lacnic.net/honeynet].

Técnicas de mitigação

Na nossa segunda parte partilhamos algumas técnicas reativas contra ataques de DDoS, que são úteis para mitigar os danos ou o impacto quando estes ocorrem.

Quando a organização é vítima de um ataque de DDoS, o seu impacto será minimizado se:

1) A organização dispõe de ferramentas para detectar e controlar os ataques de DDoS.

2) A organização tem um plano de mitigação para esse tipo de ataques. Este plano deve definir como proceder para: estar preparados, identificar o ataque, conter, remediar e recuperar. Para cada uma destas etapas, recomenda-se a definição de procedimentos relacionados a serem realizados:

   a) **Preparação** • contatos e procedimentos • ISP e suporte especializado • configurações de rede e infraestrutura

   b) **Identificação** • detecção e alerta • análise de ataque • identificação de motivação • aquisição/refinamento da mitigação • rastreamento

   c) **Contenção** • modificações da rede • controle de entrega de conteúdo • controle de tráfego

   d) **Correção** • priorização e bloqueio da largura de banda • depuração do tráfego (traffic scrubbing) • sinkholing

   e) **Recuperação** • verificação do status normal • reversão (rollback)

   f) **Lições aprendidas** • revisão do incidente e divulgação de informações • aplicação da lei