Best Practices and Techniques for DDoS Attack Mitigation

Author: Graciela Martínez
Coordination and Revision: Communications Area
Edition: Communications Area
Department: Technology Area

September 2024

lacnic
www.lacnic.net

DDoS attacks exploit vulnerabilities in the various layers of the TCP/IP stack or overwhelm a network's capacity to handle large volumes of traffic. This is why it is important for organizations to implement comprehensive protection. In this report, we share with the community several actions that can complement a DDoS solution and protect both servers and networks.

This first part outlines the main actions an organization can take to prevent DDoS attacks (either by lowering their likelihood and/or by minimizing their impact).

To enhance network and service configuration to reduce the likelihood of DDoS attacks and strengthen our infrastructure against them, if feasible, it is advisable to implement the following:

1. **Redundancy and load distribution**:

   Use CDNs to protect websites. CDNs are distributed networks of proxy servers that reduce latency by caching content and bringing it “closer” to end users. This means DDoS attacks will be mitigated closer to their source, limiting their impact on performance.

2. **Rate limiting**:

   Restrict the number of requests a user can make within a certain time frame to prevent abuse.

3. **Traffic filtering**:

   Configure firewalls and intrusion detection systems (IDS) to filter out malicious traffic based on known patterns and signatures, as well as by applying machine learning.

4. **Anycast routing**:

   Use Anycast routing to distribute traffic across multiple locations, making it more difficult for attackers to focus their attack on a single target.

5. **Overload capacity**:

   Make sure the infrastructure can handle significant traffic surges by using additional servers and increased bandwidth.

6. **Protocol-level protection**:

   Properly configure network protocols to mitigate vulnerabilities that may lead to amplification attacks and thus minimize their impact.

As for monitoring and detection, best practices include:

7. **Early detection and response systems**:

   Implement monitoring solutions that detect unusual traffic patterns and automatically respond to potential attacks.

8. **Implement mechanisms to:**

   - Detect malicious bots and block their traffic without disrupting legitimate users.
   - Implement mechanisms to distinguish between attack traffic and legitimate traffic.

   While differentiating attack traffic from legitimate traffic can be challenging, various tools, projects, and initiatives are available to help identify possible unwanted traffic patterns.

Mitigation techniques

In the second part of this report, we share some reactive techniques against DDoS attacks that can help mitigate their impact when they occur.

When an organization is the victim of a DDoS attack, the impact will be minimized if:

1) The organization has tools in place to detect and control DDoS attacks.

2) The organization has a mitigation plan for this type of attack. This plan should outline the steps to prepare, identify the attack, contain, remedy, and recover. For each of these stages, it is recommended to define procedures related to the following:

   a. **Preparation** • Establishing contacts and procedures • ISPs and specialized support • Configuring network and infrastructure settings

   b. **Identification** • Detecting and issuing warnings • Analyzing the attack • Identifying its motivation • Acquiring/refining mitigation strategies • Tracking

   c. **Containment** • Modifying the network • Controlling content delivery • Controlling traffic

   d. **Remediation** • Prioritizing bandwidth and blocking • Scrubbing traffic • Sinkholing

   e. **Recovery** • Verifying return to normal status • Rollback

   f. **Lessons learned** • Reviewing the incident and disseminating information • Law enforcement