25. MODERN METHODS OF PROTECTION AGAINST DDOS ATTACKS

Sazanovich M. I., Snitko R. E

Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus

Ryabykh. V. A. – Lecturer, Master of Arts

This article presents the analysis of modern methods for protecting against distributed denial-of-service (DDoS) attacks. It examines key approaches to mitigating their impact, including traditional protection methods and cutting-edge technologies such as cloud platforms, machine learning algorithms, and adaptive monitoring systems.

The importance of securing IT infrastructure in the digital era cannot be overstated as cyber threats are constantly changing. One major threat is Distributed Denial of Service (DDoS) attack that floods a system's resources with high traffic causing the services to become inaccessible [1]. Whereas traditional DoS attacks are single-source, DDoS attacks are multiple-source attacks, making them more difficult to detect and prevent. User devices such as computers and Internet of Things devices are usually infected by a botnet and hacked by hackers to generate malicious traffic.

There are different types of DDoS attacks that target different areas of the target infrastructure. A typical one is a massive attack that attempts to increase the bandwidth of the victim's network by overflowing this data stream with excessive traffic (UDP attacks using the user datagram protocol). This leads to network overflow, waste of resources, and blocking the processing of legitimate traffic. Protocol attacks exploit vulnerabilities in network protocols such as the SYN flood attack. In this case, the attacker sends a huge number of requests to the server. Application-level attacks: Applications target the application layer of the system. These attacks simulate legitimate traffic, such as HTTP streams, in order to overload server resources. They do not know that they have been activated, and although they appear to be normal traffic, they can consume a lot of resources, causing a delay or malfunction of the system.

It is necessary to keep developing new methods for DDoS mitigation, to implement them, to provide both traditional and cutting-edge protection from DDoS attacks [2]. The major approach is traffic filtering, the process of examining and rejecting suspicious packets based on predefined variables such as IP addresses, protocols, or packet types. This not only mitigates the threat, it allows genuine traffic to flow uninterrupted. Another technique that plays a significant role is rate limiting control, limiting the number of requests to a server and not allowing the system to be flooded with too many requests at once.

Similarly, network firewalls and the IPS (intrusion prevention system) are effective at detecting malicious traffic by known attack patterns and blocking them accordingly. In your organisation, firewalls and IPS devices protect internal networks from external threats. Cloud-based solutions such as AWS Shield, Cloudflare, and Akamai offer scalable solutions for the online presence by diverting a large volume of traffic across thousands of servers, forcing the attack traffic to be absorbed, thereby reducing the impact on the on-premises infrastructure. Machine Learning (ML) and Artificial Intelligence (AI) enhance DDoS detection by analyzing network traffic patterns, identifying anomalies, and distinguishing between legitimate and malicious activity in real time. AI-driven models continuously adapt to evolving attack vectors, enabling automated threat classification, mitigation, and proactive defense mechanisms [3].

Effective protection also entails integrating with ISPs and cybersecurity services to quickly filter traffic and prevent malicious packets from reaching critical infrastructure. Defensive techniques such as traffic distribution and load balancing help mitigate the effect on main services in the event of an attack. Additionally, real-time threat intelligence sharing between organizations enhances early attack detection and response capabilities. Implementing AI-driven traffic analysis further improves accuracy in distinguishing between legitimate and malicious requests, reducing false positives and optimizing mitigation strategies.

The final note to prevent DDoS attacks requires a multifaceted solution that leverages cloud-based solutions, machine learning, and hybrid defense systems. Robust infrastructure is key to mitigating new waves of attacks, incorporating regular updates, threat intelligence, ISPs, and external experts. Additionally, implementing real-time monitoring and automated incident response mechanisms helps detect and neutralize threats before they cause significant damage. Collaboration with global cybersecurity networks further strengthens defense strategies by sharing insights on emerging attack patterns and mitigation techniques.

References:

1. Bhattacharyya, D. K., Kalita, J. K. DDoS Attacks: Evolution, Detection, Prevention, Reaction, and Tolerance : Databook / Chapman and Hall/CR. – 2016, p. 283.

2. Mirkovic, J., Reiher, P. A taxonomy of DDoS attack and DDoS defense mechanisms : Manual / ACM SIGCOMM Computer Communication Revie. – 200., 34(2), p. 39–53.

3. Wang, H., Jin, C., Shin, K. G. Defense against spoofed IP traffic using hop-count filtering : Databook / IEEE/ACM Transactions on Networking. – 2007. 15(1), p. 40–53.