CLOUDFLARE®

DDoS mitigation from Cloudflare

Ashkan Zahabiuon, Benjamin Taylor, Aaron Sowah

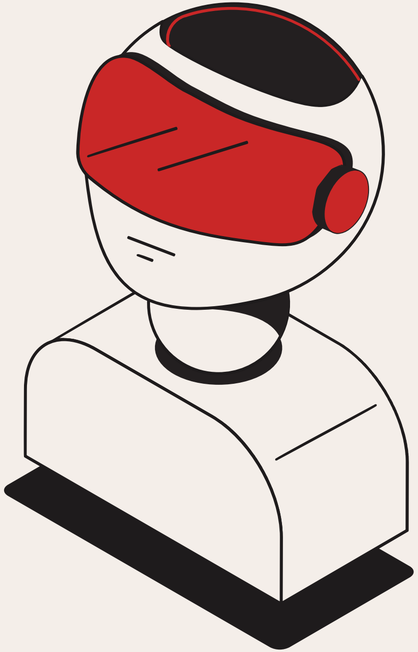
ITCS-3166-001 // Group 9

01

Understanding DDoS and Cloudflare's Response

Understanding DDoS Attacks

- DDoS (Distributed Denial of Service) attacks aim to make online services unavailable by overwhelming them with traffic from multiple sources
- Why It Matters: It’s crucial for businesses to defend against these attacks to maintain service availability and safeguard sensitive data



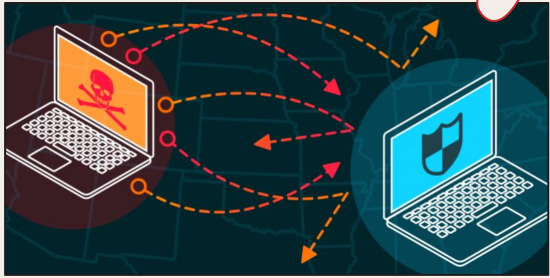
What is Cloudflare?

- Cloudflare is an international company offering a broad suite of online security/performance solutions.
- It runs a global network of servers designed to improve speed, reliability, and protection or digital assets.

Rise of DDoS Attacks

- Over the last decade, DDoS attacks have grown more frequent, massive in scale, and increasingly difficult to counter
- A significant example is the 2016 Mirai Botnet attack, which hit DNS provider Dyn, causing widespread outages on major websites

Background on DDoS and Cloudflare



02

Mitigation Techniques & Real-World Efficacy

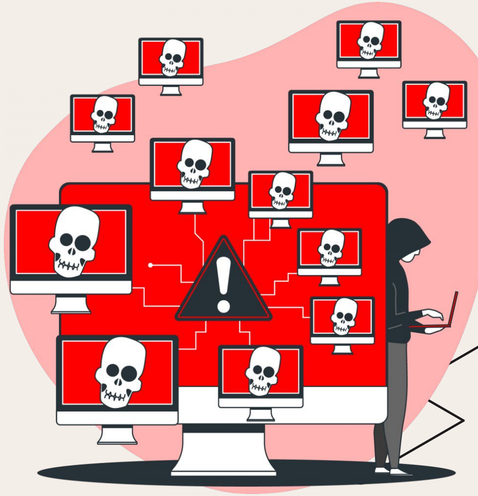
How Cloudflare's DDoS Mitigation Works

Anycast Network

- Distributes incoming traffic across a global network of servers, preventing any single server from becoming overwhelmed.
- **Example:** In the event of a DDoS attack, malicious traffic is routed to the nearest data center to handle and absorb the load.

Web Application Firewall (WAF)

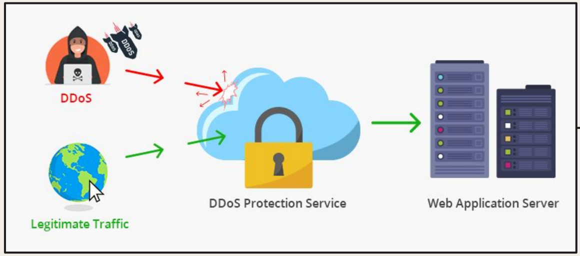
- Examines incoming requests based on predefined rules to filter out malicious traffic.
- Continuously updated to adapt to new and evolving threats.



Detailed Mitigation Process

Detection

- Cloudflare employs machine learning and real-time monitoring to detect unusual traffic patterns that may indicate a DDoS attack.
- **Example:** Sudden surges in traffic from unexpected regions or repeated hits to a single endpoint.



Mitigation

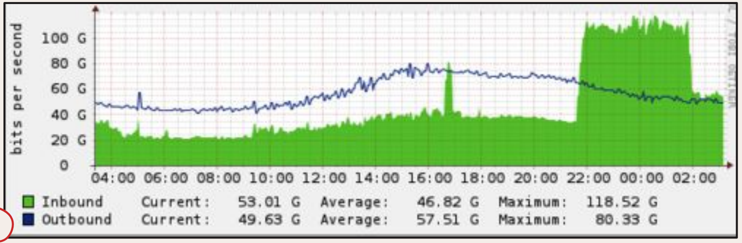
- **Rate Limiting:** Limits the number of requests a single IP can make within a set time frame.
- **Challenge-Response:** Implements CAPTCHAs to distinguish humans from bots.
- **Traffic Filtering:** Prevents access from IPs flagged for malicious activity.

Response

- **Immediate Alerts:** Notifies clients in real time about active attacks.
- **Post-Attack Analysis:** Generates comprehensive logs and detailed reports for review and investigation.

Real-World Case Study: Spamhaus Attack

- In 2013, the Spamhaus Project was hit by one of the most powerful DDoS attacks in history, peaking at 300 Gbps. Cloudflare stepped in to mitigate the attack by leveraging its global network to distribute and absorb the malicious traffic.
- Thanks to Cloudflare’s defenses, the attack was neutralized and Spamhaus remained operational and unaffected, demonstrating Cloudflare’s capability to handle even the most severe threats.
- Another case involved a government website during a crucial national election, where the website became the target of DDoS attacks designed to interrupt the election process. Cloudflare’s advanced protections ensured the site remained fully operational and ultimately upheld the election process despite the ongoing attacks.



SPAMHAUS

03

Future Trends in DDoS Mitigation and Future Outlook

Advantages & Disadvantages

Advantages

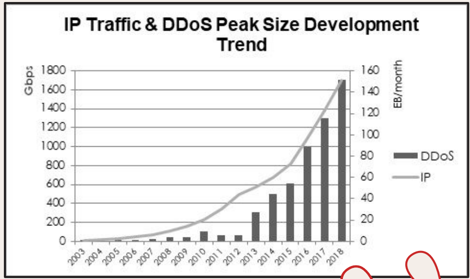
- 🌐 **Scalability:** Can handle attacks exceeding 100 Tbps
- ⚡ **Low Latency:** Ensures minimal disruption to legitimate traffic
- 🌍 **Global Coverage:** Over 200 data centers worldwide provide fast reliable mitigation

Disadvantages

- 🚫 **False Positives:** Legitimate traffic may sometimes be blocked
- 💰 **Cost:** Advanced plans may be expensive for small businesses
- ⚠ **Dependency:** Businesses relying solely on Cloudflare may face issues if Cloudflare's service is disrupted

Adoption And Usage

Cloudflare's DDoS protection services are extensively utilized across diverse sectors including e-commerce, finance, healthcare, and education.



Adoption Drivers:

- Growing frequency of DDoS attacks heightens demand for strong protection solutions like those offered by Cloudflare.
- Cloudflare’s solutions seamlessly integrate with existing IT infrastructures.

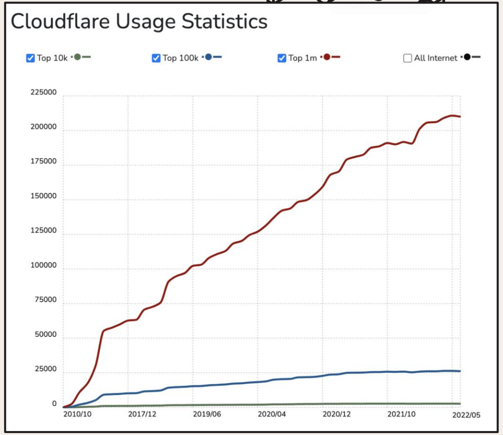
Barriers

- High costs for advanced features can be a barrier for smaller businesses.
- Many people wrongly assume that smaller websites are unlikely targets for DDoS attacks, leading to a lower perceived need for protection.

Despite these barriers, Cloudflare protects over 25 million websites and processes 45 million HTTP requests every second.

Future Predictions

Looking ahead, DDoS mitigation technologies, including those deployed by Cloudflare, are expected to evolve in response to increasingly sophisticated cyber threats.



AI-Powered Defense

Machine learning will enhance traffic analysis to detect more sophisticated attacks.

Zero-Trust Architectures

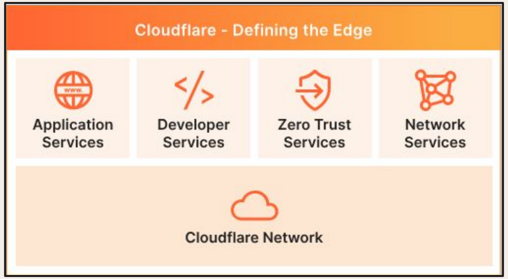
Cloudflare is likely to implement stricter access controls to prevent unauthorized traffic.

Integration with IoT

As IoT devices become common DDoS vectors, Cloudflare will likely expand protections for IoT networks.

The Future of Cybersecurity with Cloudflare

- **Effective Mitigation:** Cloudflare's advanced DDoS mitigation strategies utilize Anycast networks & AI-driven processes to defend against large-scale DDoS attacks
- **Case Study Insight:** The 2013 Spamhaus attack shows Cloudflare's ability to handle extreme cyber threats, ensuring continuity and security for critical operations



Cloudflare - Defining the Edge

Application Services

Developer Services

Zero Trust Services

Network Services

Cloudflare Network

- **Adoption & Challenges:** While Cloudflare's solutions are widely adopted across multiple industries, cost and misconceptions about DDoS risks prove to be challenges for smaller sites still
- **Strategic Importance:** Cloudflare continues to innovate (adopting zero-trust architectures and integration with IoT) which points towards a positive future in adapting to the evolving cybersecurity landscape

References & Sources

- https://cybernews.com/security/ddos-attacks-explained/
- https://www.datafoundry.com/ddos-attacks-what-are-they-and-how-can-you-be-prepared/
- https://www.nameshield.com/en/glossary/ddos-attack/
- https://www.cloudflare.com/
- https://www.gemini.com/cryptopedia/what-is-ddos-attack
- https://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho/
- https://cwatch.comodo.com/blog/cyber-attack/top-10-ddos-protection-companies/
- https://nsfocusglobal.com/ddos-in-the-past-decade/
- https://kinsta.com/cloudflare-market-share/
- https://www.cloudflare.com/what-is-cloudflare/
- https://en.wikipedia.org/wiki/Cloudflare