DDoS Mitigation

Security Lab 8

Ana Herrera Flores

Fundamentals of Information Security: Cybersecurity (88252)

Table of Contents

Introduction

In 2016, the first significant DDoS attack took place, as malicious individuals took control over 145,607 IoT devices to inundate a French web hosting server with 1.1 terabits of information per second. After that, bigger attacks have taken place. Organizations impacted by such incidents may experience financial setbacks, operational disruption, and, most critically, harm to their reputation. Businesses must respond swiftly when such events occur, and even more so, they should fortify their networks to prevent these incidents as much as possible.

What is a DDos Attack?

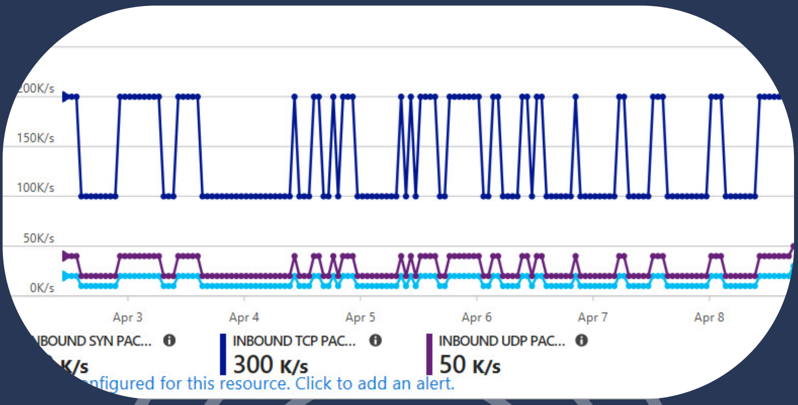
A DDos attack is a calculated cyber attack that consists in flooding a network, application or service with a massive amount of data in an attempt to take the service offline, so legitimate users cannot access it. There are three main categories: volumetric, TCP state-exhaustation, and Application-layer attack.

DDos Mitigation Techniques and Technologies

If DDos attacks cause so much hard for organizations, how do organizations attempt to mitigate a sudden DDoS attack directed at their web servers? There are different techniques that and tools that enterprises implement to protect their services:

- Traffic Monitoring to detect anomalies.

Monitoring the network to know what is the usual behavior and what is an unusual pattern. Inspection and management of network traffic to detect and prevent harmful requests from accessing the intended server or application. By adopting this proactive strategy, the effect of DDoS attacks can be avoided, as it reduces the amount of harmful traffic directed to the target.

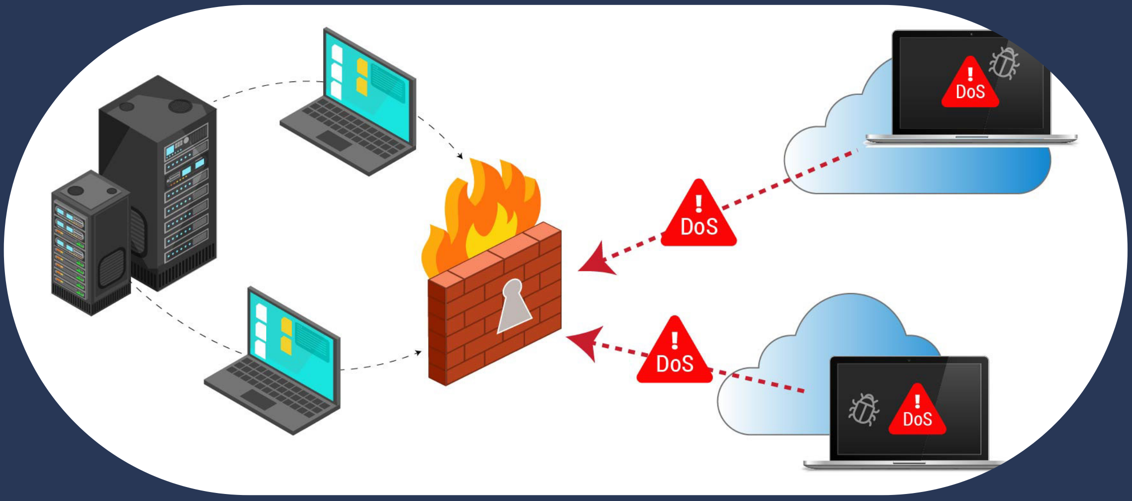


Azure DDos Protection Feature

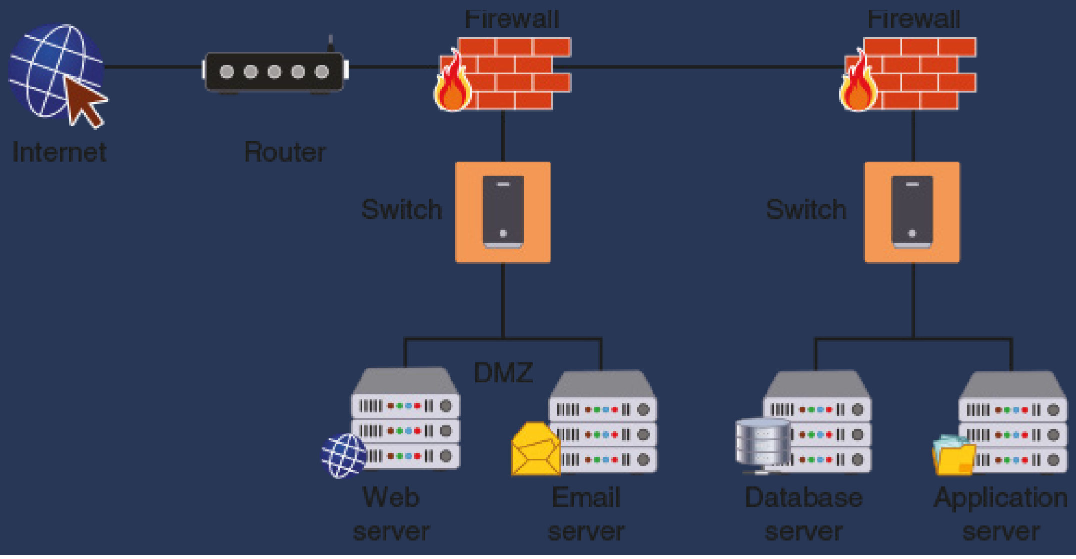
DDos Mitigation Techniques and Technologies

- Firewalls and intrusion prevention systems to filter malicious activity.

Firewalls and routers can be configured to filter IP addresses and to rate limiting.



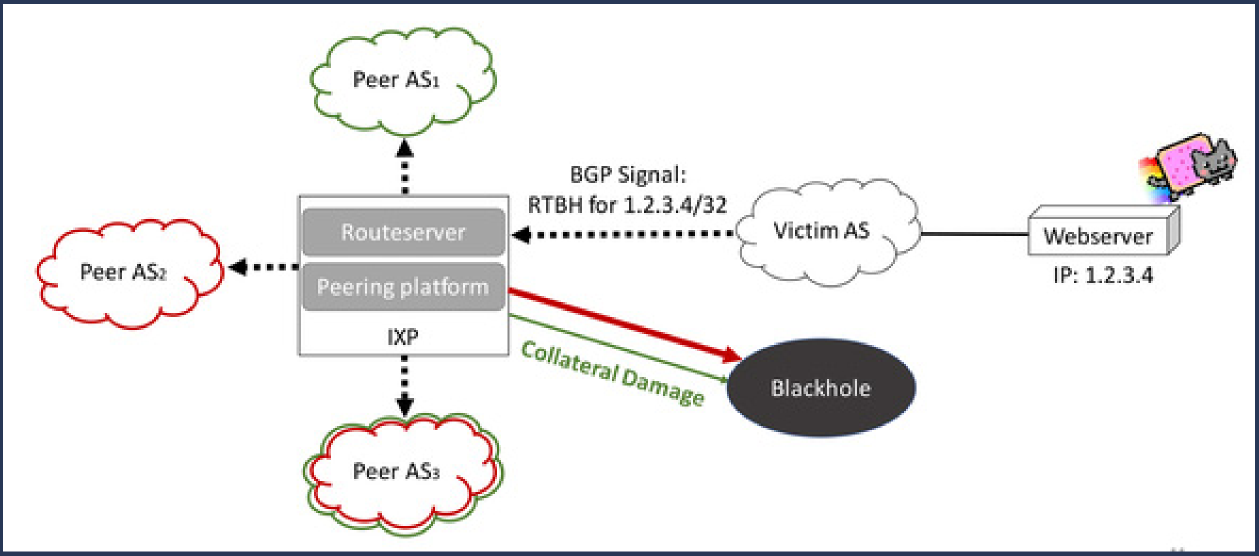
Another approach is to have two firewalls, making it harder for attackers to reach the network



DDos Mitigation Techniques and Technologies

- Sinkholing/Blackholing.

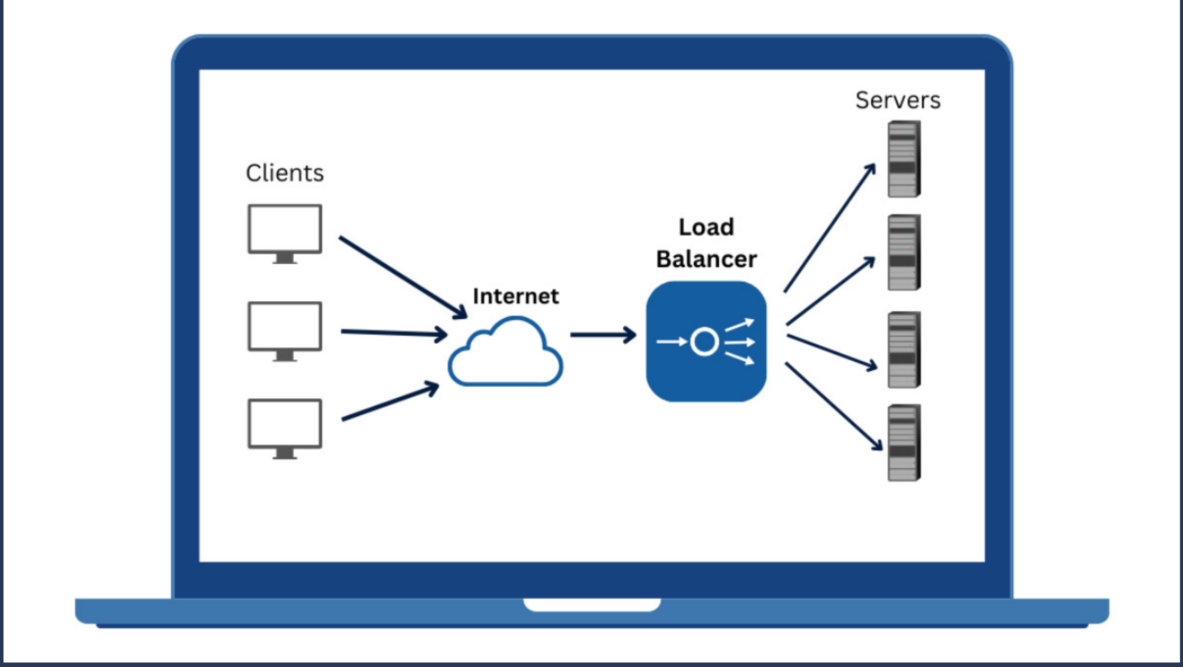
Sending the malicious activity to a black hole or sinkhole, eliminating that hostile traffic. Blackholing eliminates all traffic aimed at a particular IP address, essentially sending it into a “black hole” where it gets discarded. In contrast, sinkholing directs harmful traffic to a managed server (the “sinkhole”), enabling analysis and filtering, which may allow legitimate traffic to go through.



DDos Mitigation Techniques and Technologies

- Load balancers.

Network device or software that allocate traffic among various servers, ensuring no single server is overwhelmed, enhancing the overall performance of applications. This is accomplished by effectively managing incoming traffic across multiple backend servers.



DDos Mitigation Third-party companies

- Amazon Web Services (AWS): provides AWS shield, service for protecting AWS resources from DDoS attacks, and AWS WAF for layer 7 protection.
- Imperva: Focuses on large-scale DDoS defense, delivering fast protection from significant attacks.
- Radware: Offers instant, automated protection against DDoS with enhanced detection and response abilities.
- Cloudfare: Delivers traffic filtering, rate limiting, and WAF capabilities.

Conclusion

There are a great number of techniques, technologies and companies that enterprises can use to protect themselves against DDos attacks. Still, attackers can cause significant outages on websites, applications and services if their attack is successful. Companies should always have the latest updates and versions running on their devices, plus all the minimum cybersecurity standards. Additionally, having a cybersecurity team or an external service to oversee the network and safeguard it during an attack.

Bibliography

- Geeks for Geeks - blog. "https://www.geeksforgeeks.org/system-design/what-is-load-balancer-system-design/".

- What is DDos Attack - NETSCOUT.

- Okta. "https://developer.okta.com/books/api-security/dos/how/".

- Exacrypt security. "https://exacrypt.net/the-power-of-sinkholing-against-ddos-attacks/#:~:text=Sinkholing%2C%20also%20known%20as%20“black,impacting%20the%20target%20network's%20resources."

- CompTIA Security+ Guide to Network Security Fundamentals - Mark Ciampa