****

**“AZƏRBAYCAN HAVA YOLLARI” CJSC**

**NATIONAL AVIATION ACADEMY**

**Topic**: DDOS prevention. Cloudflare

**Subject**: Operating Systems

**Teacher**: Mammad Sahmaliyev

**Group**: 2450i

**Student**: Alakbarova Rahimakhanim

**Date**: 14.11.22

**Signature**: Alakbarova Rahimakhanim

**Baku 2022**

Distributed denial of service (DDoS) attacks are on the rise and have evolved into complex and overwhelming security challenges for organizations. Although DDoS attacks are not a recent phenomenon, the methods and resources available to conduct and mask such attacks have dramatically evolved. A milestone in the evolution of DDoS attacks is the formation of the Mirai botnet; this botnet consisted of over 300,000 hacked IoT devices used to generate the current largest known DDoS attack, with peak attack traffic exceeding 1 Tbps of throughput. According to Cloudflare’s experience, anybody - large and small organizations - can be targeted. Even though many jurisdictions have laws under which DDOS attacks are illegal, there are DDOS-as-a-Service providers offering subscriptions, some starting as low as at $5 - $10/month. Lost revenue is only one of the many threats that these kinds of attacks can bring upon your website or business. DDoS impacts such as site inaccessibility brings about less quantifiable losses, such as brand degradation and worsening customer satisfaction.

**A Scalable and Precise**

DDoS Solution Cloudflare’s global Anycast network has a network capacity of over 37 Tbps which is over 30x bigger than the largest DDoS attack ever recorded, allowing all internet assets on Cloudflare’s network to withstand massive modern-day DDoS attacks. Cloudflare’s DDoS protection for layers 3, 4, and 7 is delivered through every one of Cloudflare’s 200+ data centers globally available at the network edge. Legacy DDoS protection solutions are based on scrubbing centers which act as ‘choke-points’, introducing latency and manual intervention in the face of sophisticated DDoS attacks. Cloudflare’s unique and modern distributed architecture is built to the scale of modern-day threats, and can be used to mitigate DDoS attacks of all forms and sizes. Rate Limiting complements Cloudflare’s DDoS protection by allowing for precise mitigation of the most sophisticated attacks against the application layer.

**Predictive Security**

Cloudflare provides an automatic learning platform, where network traffic is analyzed in real time to identify anomalous or malicious requests. Over 1 billion unique IP addresses pass through Cloudflare’s network every day, which enables us to continuously enhance our IP reputation database and deliver comprehensive DDoS protection. In addition, we harness the full power of Cloudflare’s threat intelligence curated through machine learning models that continuously learn from the vast amount of traffic from over 27 million Internet properties protected by Cloudflare. Once a new attack is identified, Cloudflare automatically starts to block that attack type for both the particular website and the entire community.

**Flat-Rate Bandwidth Pricing**

Cloudflare provides unlimited and unmetered enterprise-grade DDoS protection at a flat monthly rate. Cloudflare believes that customers shouldn’t be penalized for the spike in network traffic associated with a DDoS attack. Hence we never charge for the attack traffic. With Cloudflare DDoS protection, customers can rest assured that their website will stay online and they’ll have a predictable monthly bill.

**How it works**

To detect and mitigate DDoS attacks, Cloudflare’s Autonomous Edge and centralized DDoS systems analyze traffic samples “out-of-path”, which allows Cloudflare to asynchronously detect DDoS attacks without causing latency or impacting performance.

The analyzed samples include:

* **Packet fields** such as the source IP, source port, destination IP, destination port, protocol, TCP flags, sequence number, options, and packet rate.
* **HTTP request metadata** such as HTTP headers, user agent, query-string, path, host, HTTP method, HTTP version, TLS cipher version, and request rate.
* **HTTP response metrics** such as error codes returned by customers’ origin servers and their rates.

Once attack traffic matches a rule, Cloudflare’s systems will track that traffic and generate a real-time signature to surgically match against the attack pattern and mitigate the attack without impacting legitimate traffic. The rules are able to generate different signatures based on various properties of the attacks and the signal strength of each attribute. For example, if the attack is distributed — that is, originating from many source IPs — then the source IP field will not serve as a strong indicator, and the rule will not choose the source IP field as part of the attack signature. Once generated, the fingerprint is propagated as a mitigation rule to the most optimal location in the Cloudflare edge for cost-efficient mitigation. These mitigation rules are ephemeral and will expire shortly after the attack has ended, which happens when no additional traffic has been matched to the rule.