Taming the ever-evolving DDoS monster

SYNOPSIS
The Trusted Source for Everything Cloud

CLOUDFLARE | PARTNER NETWORK

The first denial of service (DoS) was observed in 1974, when a curious teenage high school student ran a software experiment to deny computer login access to a room full of users. Since then, a small DoS experiment has evolved into a present day cyber monster - a monster that has evolved dramatically. For example, in the last decade, we have observed the creation of DDoS-for-hire websites that provide the capability of DDoS-as-a-Service for technical and non-technical users.

The 3 Ugly Heads of the DDoS Monster: Scale, Multi-vector and Ubiquity

1. SCALE

In 2016, a **Mirai Botnet DDoS** attack caught the world's attention: massive volumetric DDoS attack targeted and took down OVH, one of the largest European hosting providers. According to OVH telemetry, the attack peaked at 1Tbps and was carried out using 145,000 IoT devices.

A few years later in 2018, **GitHub** experienced one of the largest recorded volumetric DDoS attack at 1.35Tbps that employed an obscure amplification attack vector: the **memcached** protocol, which uses UDP port 1121.

Large-sized attacks are impactful; however, generating large amounts of traffic to exhaust the victim's resources is costly. Owing to this, the attack trend is shifting towards burst attacks. These are appreciably large in size but shorter in duration which overwhelms the target website but potentially goes undetected by automatic systems due to its short duration.

2. MULTI-VECTOR

DDoS attack tactics, like other security attack tactics, often exploit weaknesses in protocol communication processes. Taking the TCP protocol as an example, a DDoS attack can exhaust server resources via SYN floods or ACK floods. The existence of weaknesses like this across multiple protocols including UDP, ICMP provides an arsenal of attack tactics that malicious actors can leverage while launching a DDoS attack.

Wikipedia, for example, detected a major disruption of global user access to its sites in September 2019, for approximately 9 hours. While the web application's availability and performance was affected at the HTTP server layer, the DDoS attack directly targeted Wikipedia's data centers, at the network layer. The attack was observed to be 250+ Gbps in size and was a combination of ACK and UDP flood.

3. UBIQUITY

DDoS attacks are a sad reality for today's organizations and businesses. While companies in larger economies like the United States are lucrative targets for malicious attackers, businesses across the world experience sophisticated DDoS attacks regardless of their industry vertical. In 2019, South African Banks experienced sustained DDoS attacks that were accompanied by ransom notes, while South African telcos like Liquid Telecom fought off massive DDoS attacks that were over 100 Gbps in size.

> "Malicious actors continually explore new avenues and tactics to launch evolved DDoS attacks."

Growing Appetite of the DDoS Monster

The onset of 2020 has been marked with rampant DDoS attacks. EVE Online, a massively multiplayer online (MMO) gaming company, experienced multiple days of service disruption due to a DDoS attack. Online forums for the game were inundated with frustrated players wanting to cancel their accounts or demanding compensation because they had not been able to log in for days. For MMOs, a minor rise in response time is extremely frustrating for customers, let alone a days-long disruption.

Malicious actors continually explore new avenues and tactics to launch evolved DDoS attacks. As an example, hackers are currently attempting to scan the Internet for exposed NSC Linear eMerge E3 devices to exploit the CVE-2019-7256 vulnerability that would allow them to take over devices, download and install malware, and then launch DDoS attacks on other targets. . These devices are generally installed in corporate buildings, factories and similar infrastructure and serves as an access control system for employees and visitors.

Slay the DDoS Monster in the Cloud

Legacy approaches of employing on-premises-based hardware appliances for DDoS protection are outdated, as the DDoS attacks of today are bigger, more sophisticated, and global, and on-premises DDoS solutions fail to match against the scale, velocity, and distributed nature of the attacks.

However, the distributed architecture of cloud-based DDoS protection solutions provide an always-on posture to mitigate DDoS attacks globally. It is vital to consider the following aspects while selecting a cloud-based DDoS protection solution:

DISTRIBUTED ARCHITECTURE

The global nature of DDoS attacks requires that the DDoS protection solution have a globally distributed architecture in order to mitigate the attacks as close as possible to the attack source. As the size of the DDoS attacks has increased, legacy scrubbing center approach for cloud-based DDoS solutions has quickly become obsolete. It's owing to the 'choke-point' nature of scrubbing centers. Traditionally, DDoS solution providers have invested in a small number of scrubbing centers to which large-sized DDoS attacks need to be diverted to, as they do not have a truly distributed architecture.

Learn more about the shortcoming of a scrubbing center approach through this excellent blog - 'No **scrubs**.'

Cloudflare's modern DDoS protection solution runs as a service on every server across all of its data centers in 200 cities globally, making it a truly distributed DDoS solution. When a DDoS attack originates in any corner of the world, it is mitigated at the closest Cloudflare data center, allowing for faster mitigation of the attack and higher uptime for customers' infrastructure.

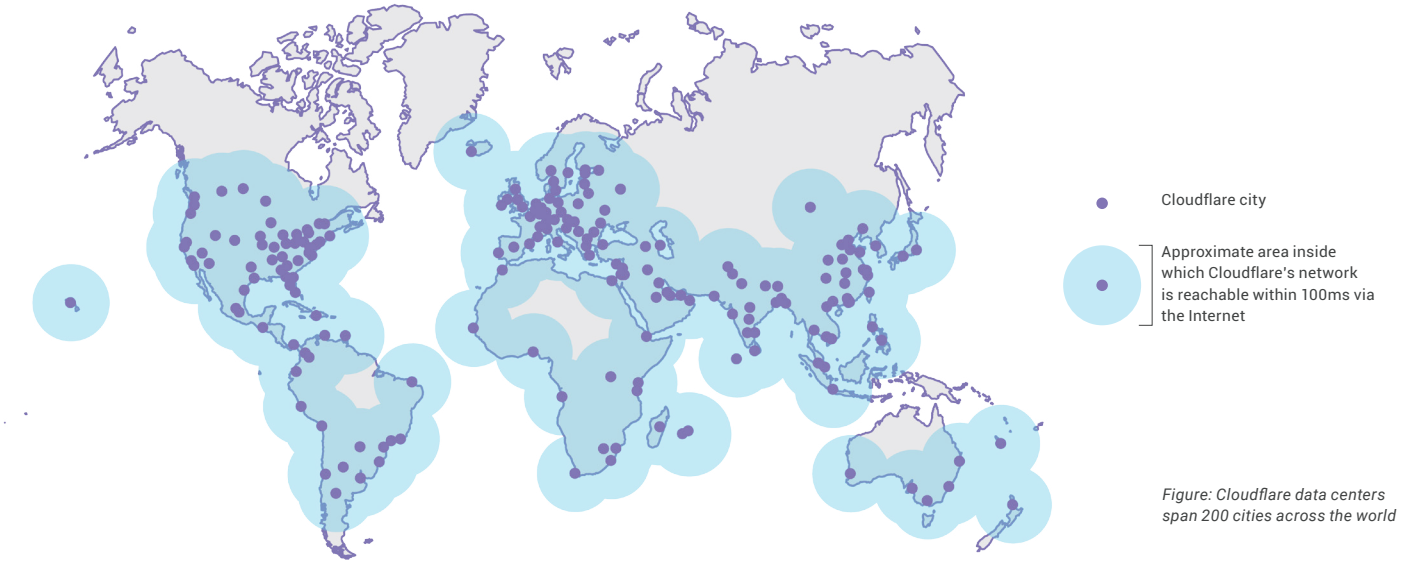


Figure: Cloudflare data centers span 200 cities across the world

NETWORK CAPACITY

To squash the scale and size of the DDoS attack, the DDoS protection solution's network capacity plays a pivotal role, especially with DDoS attacks ranging in the Tbps scale.

Cloudflare's Anycast global network has a network capacity of over 30 Tbps, which allows it to mitigate even the largest DDoS attacks. Additionally, Cloudflare is connected to more Internet exchange points than other providers worldwide. Cloudflare's network interconnects with over 8,000 networks globally, including major ISPs, cloud services, and enterprises.

COMPREHENSIVE COVERAGE

There is an entire arsenal of attack tactics that malicious actors can leverage while launching a DDoS attack at the application and network layers. Cloud-based DDoS solutions should have the capability to comprehensively mitigate DDoS attacks at multiple layers.

Cloudflare's advanced DDoS protection provides comprehensive coverage against layer 7 DDoS attacks, while Cloudflare Spectrum and Magic Transit mitigate DDoS attacks at layers 3 and 4. ThousandEyes' **blog** on the analysis of the DDoS attack against Wikipedia, highlights how Cloudflare was able to quickly and comprehensively mitigate a multi-vector large DDoS attack.

REAL-TIME INTELLIGENCE

Instead of being in a reactive mode, DDoS protection solutions should be fortified with real-time threat intelligence to develop a proactive posture for mitigating DDoS attacks.

Cloudflare's DDoS protection solution is powered by the threat intelligence gathered by its always-learning network that protects over 20 million Internet properties and inspects over 1 billion unique IPs daily. Armed with this threat intelligence, machine learning models, and engineering expertise from a battle-tested team, Cloudflare's DDoS protection provides a robust solution in the face of the most sophisticated DDoS attack.

AUTOMATED MITIGATION

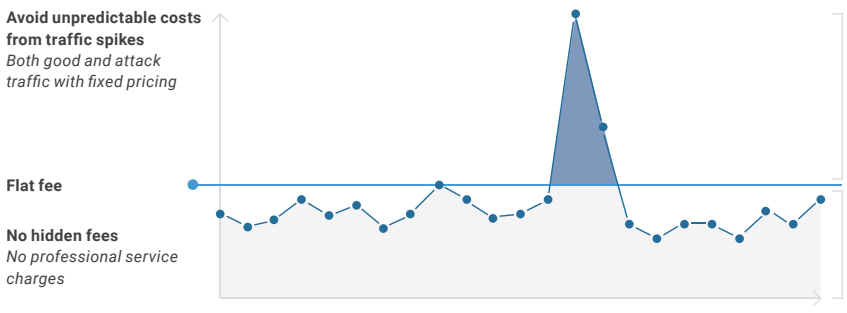
Sophisticated DDoS attacks require automated mitigation that continuously inspects traffic headed to a business (no matter whether it is based on-premises or in the cloud), applies real-time analysis, and mitigates DDoS attacks quickly.

Cloudflare's automated systems (**gatebot** and **dosd**) ontinuously analyze attack fingerprints, anomalies, rules, blacklists, and more. The gatebot system is instrumental in mitigating global volumetric attacks while the dosd system runs on every server to mitigate localized attacks. These automated systems together recommend 400K+ dynamic rules per second for fast mitigation.

COST-EFFECTIVE

As the size and scale of DDoS attacks grow, every business and organization needs to consider that the cost of the DDoS protection is sustainable. Cloud DDoS protection solution providers often employ a metered DDoS protection. While cloud-based solutions provide a superior protection solution as compared to on-premises-based solution by elastically scaling to protect against a DDoS attack, the metered mitigation can often result in a massive spike in billing. Rather than losing money on unserviced customers, a business can potentially be crippled by the metered costs of mitigating the DDoS attack.

Cloudflare offers **unlimited and unmetered** DDoS mitigation. This eliminates the legacy concept of 'Surge Pricing,' which is especially painful when a business is under duress and experiencing a DDoS attack. This enables you to avoid unpredictable costs from traffic spikes.



Be a hero — **slay the DDoS monster** today!

+973 1655 5000 | info@synopsis-tech.net | www.synopsis-tech.net