DDoS Protection with Cloudflare

The Evolution of Modern Day DDoS Attacks

2016
1 Tbps
IoT Botnet Layer 7 Attack

Largest Layer 7 attack ever seen using Mirai IoT botnet. Attack was both volumetric and utilized server resources.

2014
400 Gbps
NTP Amplification Attack

An attacker used 4,529 NTP servers to amplify an attack from a mere 87 Mbps source server

2013
120 Gbps
Layer 3/4 DDoS Attack

Spamhaus attack was considered one of the largest at that time, and was labeled "the attack that almost broke the internet."

.

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. Attacks of this magnitude are becoming the new standard.

DDoS attacks are often not one off events and victims are typically targeted multiple times in a year. 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. Even Amazon's website ($99 Billion in retail revenues in 2015) went down multiple times in the past for unknown reasons. For example, in 2013 Amazon.com went down for an estimated 15-45 minutes, costing the company $1.8 - $5.3 million in lost sales, based on the company's average sales of $117,882 per minute. In addition, things like site inaccessibility brings about less quantifiable losses, such as brand degradation and worsening customer satisfaction.

A Scalable and Precise DDoS Solution

A Cloudflare's 10 Tbps global anycast™ network is 10x 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 available as a service at the network edge, matching 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.

PROTECTION AGAINST LAYER 3 & 4 DDOS ATTACKS

Layer 3 and layer 4 DDOS attacks are usually volumetric attacks such as DDoS amplification, DDoS flood and DDOS SYN flood attacks. While those attacks can overwhelm a typical unicast based network, Cloudflare's Anycast based network inherently increases the surface by spreading the attack traffic to each of the more than 102 Cloudflare datacenters and to a diverse set of high bandwidth interconnections with other networks, to simply absorb the attack traffic.

DDoS Protection Features

- Layers 3, 4, and 7 DDoS protection
- DNS attack protection
- Fine-grain threat blocking with Rate Limiting
- Predictive security with IP reputation database

"Knowing that we don't have to worry about DDoS attacks against our API and gateway servers gives us the peace of mind to focus on improving our product."

-Jake Heinz, Software Engineer at Discord

Cloudflare's Network

- Global Anycast™ network of 102+ data centers
- 10 Tbps throughput to absorb volumetric attacks
- 6 million Internet properties
- Flat-rate bandwidth pricing

"The reason we use Cloudflare is because the security features are excellent, the CDN is high performing, and it's really convenient that these solutions are packaged together. It makes managing everything easy, and allows us to focus on our core business."

-Amanda Kleha GM, Zendesk Online Business Unit

PROTECTION AGAINST LAYER 7 APPLICATION VULNERABILITIES

Common types of Layer 7 attacks include SQL injection and Cross-Site Scripting (XSS), which might allow attackers to access and temper with customer or any other kind of application data. Cloudflare addresses these threats via its Web Application Firewall (WAF). The WAF automatically blocks threats found in the OWASP top 10 rule set, Cloudflare's application rule sets, as well as custom rules created by the community/ customers. Cloudflare has been able to protect their customers against major zero-day vulnerabilities, including the Shellshock vulnerability and the Heartbleed Bug.

RATE LIMITING

Activate Cloudflare Rate Limiting for fine-grained traffic control that complements Cloudflare's DDoS protection and web application firewall (WAF) services. Rate Limiting protects against denial-of-service attacks, brute-force password attempts, and other types of abusive behavior targeting the application layer. Configure request thresholds, define custom responses, such as mitigating actions (challenges or CAPTCHAS) or response codes, and gain analytical insights into endpoints of your website, application, or API.

Predictive Security

Cloudflare provides an automatic learning platform, where network traffic is analyzed in real time to identify anomalous or malicious requests. Once a new attack is identified, Cloudflare automatically starts to block that attack type for both the particular website and the entire community. As Cloudflare continues to grow its network and its community, it will become increasingly difficult to launch an effective DDoS attack against any of Cloudflare's users.

Flat-Rate Bandwidth Pricing

Cloudflare provides unlimited enterprise-grade DDoS protection at a flat monthly rate. Cloudflare believe that customers shouldn't be penalized for the spike in network traffic associated with a DDoS attack. With Cloudflare DDoS protection, customers can rest assured that their website will stay online and they'll have a predictable monthly bill.

Sign up for Cloudflare

Sign up with Cloudflare and activate Rate Limiting to protect your website, application, or API, from DDoS attack, while reducing latency and utilizing the latest web technologies. The set up is easy and usually takes less than 5 minutes to get up and running. Check out the plans, ranging from Free to Enterprise at www.cloudflare.com.