CLOUDFLARE

EBOOK

Five critical considerations for mitigating DDoS attacks

How to protect your organization with a better DDoS defense

Table of Contents

Overview

Distributed denial-of-service (DDoS) attacks remain one of the most effective methods used by cyber criminals to cause significant financial, operational, and reputational damage to organizations worldwide. Though these attacks take different forms, the goal is always to incapacitate targeted servers, services, or networks by flooding them with traffic from organized botnets, compromised devices, or networks.

As organizations have hardened their cyber defenses, criminals have responded with newer attack types targeting multiple applications and services. Some of these attacks target the network and transport layer in new ways, resulting in record-breaking network traffic spikes of almost 6 Tbps per second. Others are low-speed, low-intensity, application layer-based offensives designed to be undetectable while targeting one or more services gateways.

Meeting the challenges associated with DDoS attacks requires a comprehensive approach that addresses all threats from the network to application layer.

But enhanced security should not compromise performance. While on-premise solutions can be part of the answer, more robust solutions integrate performance with scalable, cloud-based, as-close-to-the-source mitigation that works at the network edge to deliver maximum agility and capacity that scales.

What is a DDoS attack?

A DDoS attack is a malicious attempt to disrupt the normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

They achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices.

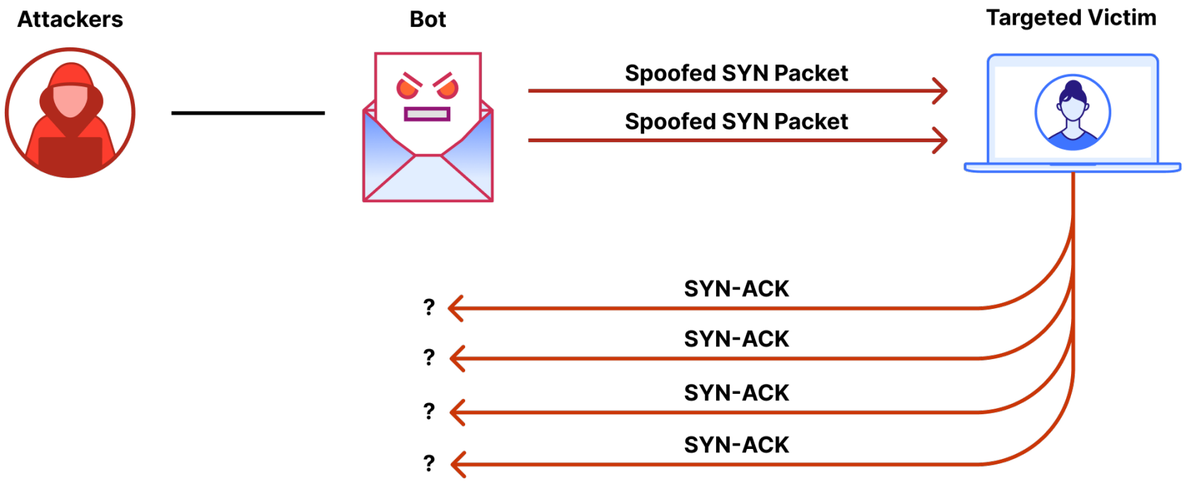
From a high level, a DDoS attack is like an unexpected traffic jam clogging up the highway, preventing regular traffic from arriving at its destination.

Types of DDoS attacks

DDoS attacks can target an organization's application, network, or origin data center at several different layers. While all of these attacks involve inundating targets with malicious traffic, they can be divided into three distinct categories:

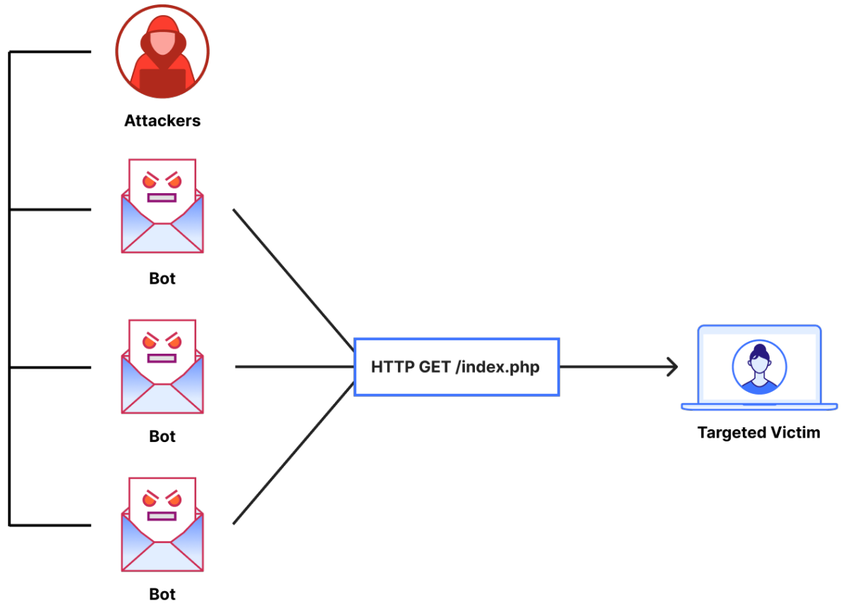
Protocol attacks:

A protocol attack targets vulnerabilities in the network and transport layers in order to consume all the available capacity of web servers or their intermediate resources — including firewalls and load balancers. These attacks can involve SYN floods and fragmented packet attacks. All of these types of attacks are measured in packets per second (PPS).



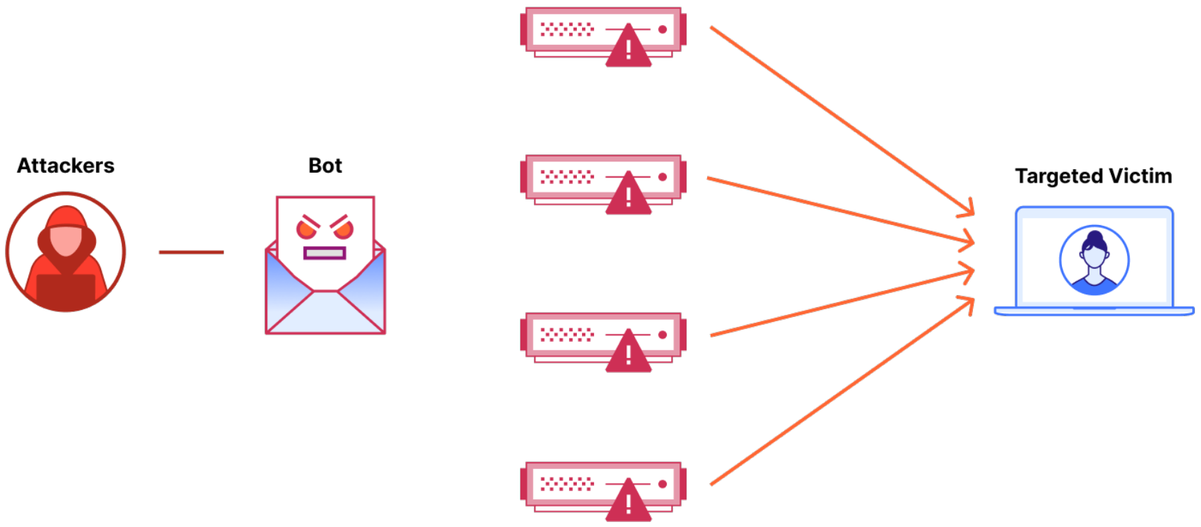
Application layer attacks:

Application layer attacks target the layer where webpages are generated on the server and delivered in response to HTTP or HTTPS requests. Akin to repeatedly hitting 'refresh' in a web browser on multiple computers simultaneously, the resulting flood of HTTP/S is measured in requests per second (RPS).



Volumetric attacks:

These volumetric attacks attempt attempt to create congestion by consuming all available bandwidth between the target and the larger Internet. Large amounts of data are sent to a target by using a form of amplification or another means of creating massive traffic, such as requests from a botnet.



Why should organizations care about DDoS attacks?

Getting knocked offline by DDoS attacks can have a detrimental impact on revenue, customer service, and basic business functions. In today's "always on" world, going offline for even a few minutes can mean you lose valuable customers, critical revenue, and your hard-earned reputation. Whether the aim is to cripple your site or network, to divert traffic to rivals, to mask the theft of corporate data, or simply to cause maximum reputational damage, DDoS attacks can impact your customers and partners just as much as your business.

On average, severe outages typically last for 77 hours and can cost organizations up to $1.9 million per hour.[1] This goes to show that it is not just the duration of the attack that can impact the bottom line, but also what it takes to recover and to earn back the trust of customers.

As shared in the Q1 2025 DDoS Threat Report, Cloudflare blocked 20.5 million DDoS attacks, representing a 358% increase in volume compared to Q1 2024. We also saw a massive increase in the amount of attacks that exceeded over 1 Tbps. These types of hyper volumetric attacks averaged out to around 8 attacks per day with the largest being a massive 6.5 terabits-per-second (Tbps) flood that matched the highest bandwidth attacks ever reported.

Generally speaking, protecting against DDoS attacks requires the ability to:

- Differentiate between traffic spikes stemming from an attack versus high user demand
- Block traffic generated by botnets without interrupting legitimate traffic
- Intelligently route remaining traffic by breaking it into manageable chunks to prevent denial of service
- Continuously analyze traffic for malicious patterns that can aid in developing adaptive, hardened defenses

Top 10 most attacked industries: 2025 Q1

1. **Gambling & Casinos** — QoQ: +4
2. **Telecommunication, Services Providers & Carriers** — QoQ: -1
3. **Information Technology & Services** — QoQ: +1
4. **Internet** — QoQ: -2
5. **Gaming** — QoQ: +1
6. **Banking & Financial Services** — QoQ: +2
7. **Cyber Security** — QoQ: +37
8. **Retail** — QoQ: -1
9. **Manufacturing, Technology & Engineering** — QoQ: +28
10. **Airlines, Aviation, Aerospace** — QoQ: +40

Want to know more about DDoS attack trends? Check out Cloudflare's latest DDoS Threat Report.

Five critical considerations for mitigating DDoS attacks

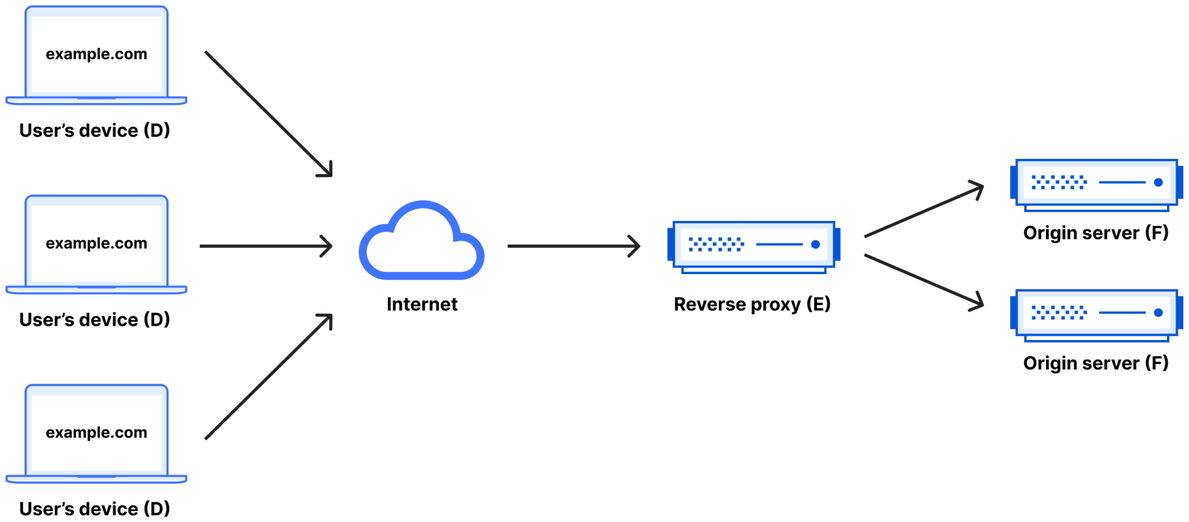
1

Tailor the approach per resource

If your objective is to protect web servers, the addition of a reverse proxy allows you to have a “front door” to your web servers that allows for additional benefits like load balancing and protection from attacks since the web servers’ IP addresses are hidden from potential attackers. The diagram shows how a reverse proxy works.

For more complex application layer attacks, a web application firewall (WAF) can act as a reverse proxy to shield targeted servers from certain types of malicious traffic.

While some organizations choose to build or deploy their own reverse proxies, this requires extensive software and engineering resources, as well as a significant investment in hardware that will need to be replaced every 3-5 years, on average.



2

Prioritize the two most important metrics: capacity and TTM

Assess your existing capacity for mitigating DDoS attacks without impacting site functionality. The traditional approach to absorbing the spikes in traffic generated by DDoS attacks has been to build out on-premise server farms. But this quickly grows costly, and even the most robust enterprise-grade infrastructure is likely to be overwhelmed in the face of volumetric attacks that grow larger by the day. Rate limiting can help, but it slows down performance and can still result in an outage if your infrastructure is overloaded.

When even a few moments of reduced availability can lead to significant lost revenue and productivity, time-to-mitigation (TTM) becomes paramount. To reduce TTM, you'll need to ensure traffic can fail over to an alternate site in the event of an outage — but that will only work for so long before your infrastructure is overwhelmed.

Here again, a more effective approach is to deploy a cloud-based mitigation solution that offers unlimited capacity to protect against DDoS attacks of any scale or complexity, and can provision services at the network edge for maximum agility in mitigating rapidly-evolving DDoS attacks.

3

Consider always-on vs. on-demand protection

DDoS mitigation services offer two primary deployment models: on-demand and always-on.

In the on-demand model, normal traffic flows directly to applications without redirection, and traffic is only diverted to cloud scrubbing centers when an attack is detected. This approach often requires customer intervention to initiate mitigation, increasing response time during attacks.

The always-on approach continuously routes all traffic through the provider's data centers for threat inspection, even during normal operations. This method offers the most comprehensive protection by minimizing detection-to-mitigation time with no service interruption required. It provides a hands-off experience as customers don't need to take action during attacks.

While always-on protection is more thorough, also make sure to verify that a potential provider will not introduce latency when diverting all traffic through their cloud infrastructure.

4

Never sacrifice performance for security

DDoS attacks cause sluggishness and outages that not only degrade performance, but also damage an organization's ability to achieve sustainable growth:

Forty-seven percent of users won't wait longer than two seconds for a website to load[2]. In other words, today's consumer expects websites and applications to load instantaneously and to never (ever) be offline.

Latency also damages productivity — time spent by employees waiting for apps to load or the network to respond can add up quickly. And the problem is compounded with the rise of remote work: 89% of respondents in one remote survey said they lost an average of just over 30 minutes a day due to slow Internet connections.[3]

Securing against DDoS without diminishing performance requires a careful balancing act.

As mentioned earlier, many organizations attempt to mitigate DDoS attacks by redirecting traffic to scrubbing centers that are usually a long distance from the traffic source or origin server. This creates a bottleneck that can result in latency levels that are just as poor as during an attack. For this reason, limited scrubbing center services are not scalable for blocking DDoS attacks that may originate from anywhere.

Instead, for faster response times, consider cloud-delivered mitigation services with the capability to perform detection and mitigation at locations physically close to an attack source in any global region.

5

Choose intelligence to stay ahead of attackers

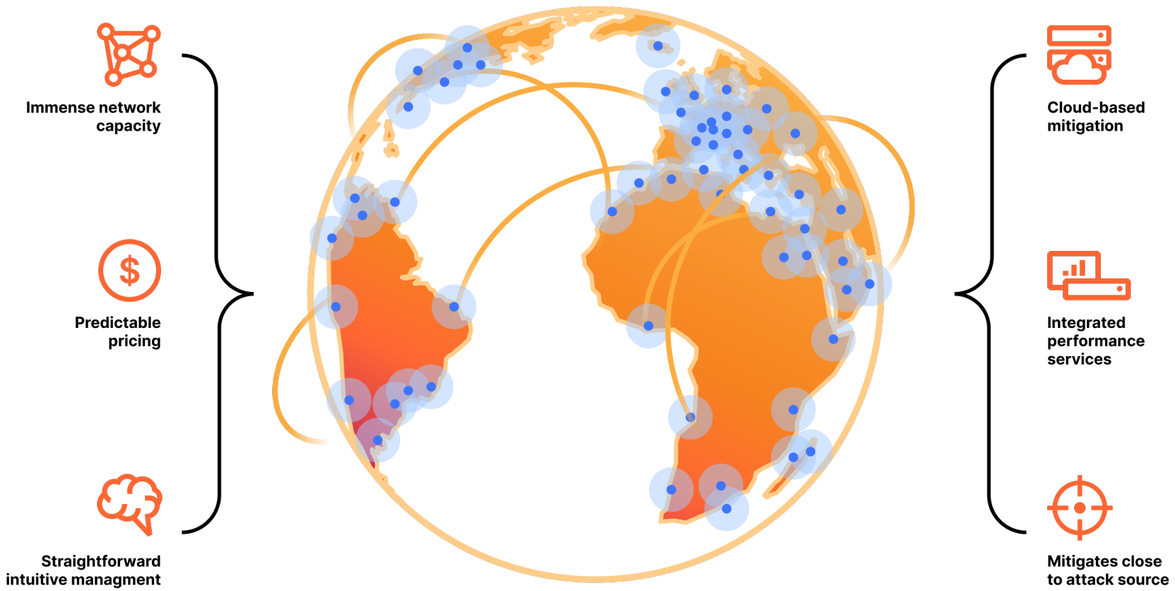
Overcoming increasingly complex DDoS attacks requires more than just a layered approach. It necessitates continual analysis of traffic for malicious patterns that can help you develop the intelligent, adaptive defenses you need to fend off future attacks.

The DDoS attack that's underway now is the secret to defeating the next: When evaluating a cloud-based mitigation service, it's important to look beyond capacity or transfer and filtering speeds, to what kind of intelligence is enabled by its reach.

The larger and more robust the mitigation network, the richer the intelligence it can provide on evolving attack patterns — and the more preemptive these services can be.

Conclusion

Meeting the challenges associated with DDoS attacks requires a comprehensive approach that addresses all threats at all layers. While on-premise solutions can be part of the answer, they can quickly get expensive and impractical. A more robust solution will integrate performance with scalable, cloud-based mitigation that provisions services at the network edge for maximum agility and unlimited capacity. Such a solution helps to ensure resilience against DDoS attacks — no matter the size or complexity.

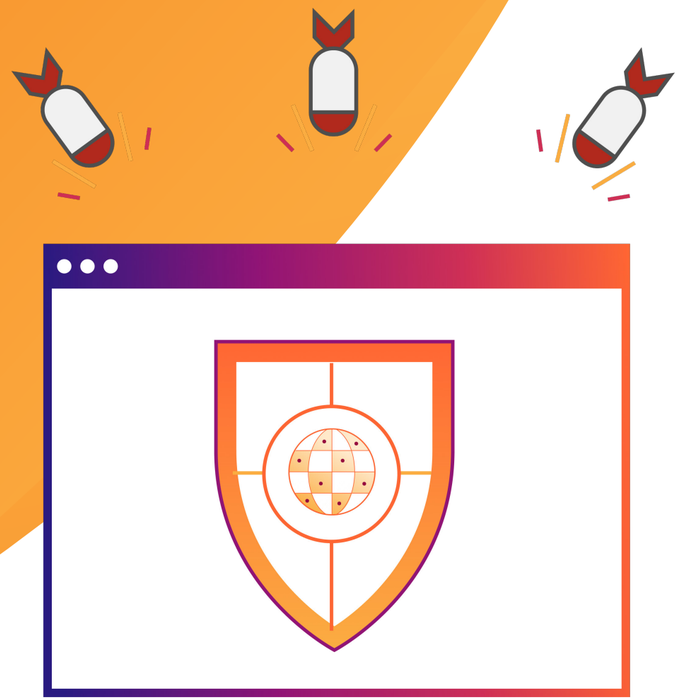


How Cloudflare helps prevent DDoS attacks

Cloudflare offers integrated L3-7 DDoS protection that helps organizations monitor, prevent, and mitigate attacks before they reach targeted applications, networks, and infrastructure. Some of the key benefits of our layered threat defense include:

- A global Anycast network that spans over 335 cities and 125 countries worldwide, capable of absorbing even the largest DDoS attacks
- Traffic routing and acceleration to help diffuse traffic spikes across our network and minimize latency and congestion
- Always-on, automatic DDoS mitigation that can detect and block malicious traffic in less than three seconds
- A next-generation WAF that offers advanced rate limiting, tailored rulesets, and flexible threat prevention

Learn how organizations like Zendesk, Shopify, and Porsche Informatik stop DDoS attacks with Cloudflare.



References

1. https://www.ciodive.com/news/it-tech-outages-cost-new-relic-report-crowdstrike/731100/
2. https://www.forbes.com/advisor/business/software/website-statistics/
3. https://www.computerweekly.com/news/252487354/Poor-connectivity-sees-home-workers-lose-over-half-an-hour-of-work-a-day

1 888 99 FLARE | enterprise@cloudflare.com | Cloudflare.com

REV:BDES-7230.2025MAY05