Reference: <https://aws.amazon.com/shield/ddos-attack-protection/>

**DDOS prevention. Cloudflare**

A Denial of Service (DoS) - *{come from one source}* attack is a malicious attempt to affect the availability of a targeted system, such as a website or application, to legitimate end users. Typically, attackers generate large volumes of packets or requests ultimately overwhelming the target system. In case of a Distributed Denial of Service (DDoS) attack, and the attacker uses multiple compromised or controlled sources to generate the attack.

In general, DdoS – *{coming from multiple sources simultaneously}* attacks can be segregated by which layer of the Open Systems Interconnection (OSI) model they attack. They are most common at the Network (layer 3), Transport (Layer 4), Presentation (Layer 6) and Application (Layer 7) Layers.

While thinking about mitigation techniques against these attacks, it is useful to group them as Infrastructure layer (Layers 3 and 4) and Application Layer (Layer 6 and 7) attacks.

Infrastructure Layer Attacks

Attacks at Layer 3 and 4, are typically categorized as Infrastructure layer attacks. These are also the most common type of DDoS attack and include vectors like synchronized (SYN) floods and other reflection attacks like User Datagram Packet (UDP) floods. These attacks are usually large in volume and aim to overload the capacity of the network or the application servers. But fortunately, these are also the type of attacks that have clear signatures and are easier to detect.

Application Layer Attacks

Attacks at Layer 6 and 7, are often categorized as Application layer attacks. While these attacks are less common, they also tend to be more sophisticated. These attacks are typically small in volume compared to the Infrastructure layer attacks but tend to focus on particular expensive parts of the application thereby making it unavailable for real users. For instance, a flood of HTTP requests to a login page, or an expensive search API, or even Wordpress XML-RPC floods (also known as Wordpress pingback attacks).

**DDoS Protection Techniques**

Reduce Attack Surface Area

One of the first techniques to mitigate DDoS attacks is to minimize the surface area that can be attacked thereby limiting the options for attackers and allowing you to build protections in a single place. We want to ensure that we do not expose our application or resources to ports, protocols or applications from where they do not expect any communication. Thus, minimizing the possible points of attack and letting us concentrate our mitigation efforts. In some cases, you can do this by placing your computation resources behind [Content Distribution Networks (CDNs)](https://aws.amazon.com/cloudfront/) or [Load Balancers](https://aws.amazon.com/elasticloadbalancing/) and restricting direct Internet traffic to certain parts of your infrastructure like your database servers. In other cases, you can use firewalls or [Access Control Lists (ACLs)](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html) to control what traffic reaches your applications.

Plan for Scale

The two key considerations for mitigating large scale volumetric DDoS attacks are bandwidth (or transit) capacity and server capacity to absorb and mitigate attacks.

Transit capacity.

When architecting your applications, make sure your hosting provider provides ample redundant Internet connectivity that allows you to handle large volumes of traffic. Since the ultimate objective of DDoS attacks is to affect the availability of your resources/applications, you should locate them, not only close to your end users but also to large Internet exchanges which will give your users easy access to your application even during high volumes of traffic. Additionally, web applications can go a step further by employing Content Distribution Networks (CDNs) and [smart DNS resolution services](https://aws.amazon.com/route53/) which provide an additional layer of network infrastructure for serving content and resolving DNS queries from locations that are often closer to your end users.

Server capacity.

Most DDoS attacks are volumetric attacks that use up a lot of resources; it is, therefore, important that you can quickly scale up or down on your computation resources. You can either do this by running on larger computation resources or those with features like more [extensive network interfaces](https://aws.amazon.com/ec2/instance-types/) or [enhanced networking](https://aws.amazon.com/premiumsupport/knowledge-center/enable-configure-enhanced-networking/) that support larger volumes. Additionally, it is also common to use load balancers to continually monitor and shift loads between resources to prevent overloading any one resource.

Know what is normal and abnormal traffic

Whenever we detect elevated levels of traffic hitting a host, the very baseline is to be able only to accept as much traffic as our host can handle without affecting availability. This concept is called rate limiting. More advanced protection techniques can go one step further and intelligently only accept traffic that is legitimate by analyzing the individual packets themselves. To do this, you need to understand the characteristics of good traffic that the target usually receives and be able to compare each packet against this baseline.

Deploy Firewalls for Sophisticated Application attacks

A good practice is to use a [Web Application Firewall (WAF)](https://aws.amazon.com/waf/) against attacks, such as SQL injection or cross-site request forgery, that attempt to exploit a vulnerability in your application itself. Additionally, due to the unique nature of these attacks, you should be able to easily create customized mitigations against illegitimate requests which could have characteristics like disguising as [good traffic](https://aws.amazon.com/blogs/security/how-to-configure-rate-based-blacklisting-with-aws-waf-and-aws-lambda/) or coming from bad IPs, unexpected geographies, etc. At times it might also be helpful in mitigating attacks as they happen to get experienced support to study traffic patterns and create customized protections.

***I have found these videoes useful, you might want to check it out:***

[***https://www.youtube.com/watch?v=ilhGh9CEIwM***](https://www.youtube.com/watch?v=ilhGh9CEIwM)

[***https://www.youtube.com/watch?v=z503nLsfe5s***](https://www.youtube.com/watch?v=z503nLsfe5s)

[***https://www.youtube.com/watch?v=iydiAoiLP8A***](https://www.youtube.com/watch?v=iydiAoiLP8A)

***------------------------------------------------------------------------------------------------***

Reference: <https://www.cloudflare.com/learning/what-is-cloudflare>

<https://www.westhost.com/>

**Cloudflare.**

Cloudflare is a global network designed to make everything you connect to the Internet secure, private, fast, and reliable.

* Secure your websites, APIs, and Internet applications.
* Protect corporate networks, employees, and devices.
* Write and deploy code that runs on the network edge.

Cloudflare is a free CDN type product that protects against threats such as SQL injection and identity theft. **Cloudflare also improves site performance and speeds up loading times by using their multiple data centers that are located around the world.** The Cloudflare network acts like a giant VPN. This means that a site visitor will access your website by being physically redirected to the closest server. What this means is simple: the closer the data center, the faster your website will load for the user. This is unique to Cloudflare.  
Another benefit is the reduction of bot crawls, which can be both helpful and harmful depending on their source. A bot crawl is typically used to go to websites and “crawl” for information on your web page. While these can be helpful when catching content thieves using your website design without permission, they can also generate false ad impressions, inject spam and malware through file backdoors, stealing website content and information. **A good way to think about Cloudflare is to think of it as a web proxy.** Because a cache of your website is available to the visitor, Cloudflare is able to block suspicious content and keep you safe from malicious viruses, spambots and harmful traffic flow.

In the early days of the Internet, when you wanted to load a website, your request would go from your computer to a server, which would then return the web page you requested.

If too many requests came in at once, that server could be overwhelmed and crash, becoming unresponsive to anyone trying to access the resources it hosted.

This made it difficult for owners of Internet properties to provide content that was fast, safe, and reliable. Cloudflare was created to ease these difficulties and empower users with the resources to make their sites, apps, and blogs safe and performant. This is done through the use of a powerful [edge network](https://www.cloudflare.com/learning/cdn/glossary/edge-server/) that provides content and other services as close to you as possible, so you get the information as fast as possible.

Einstein figured out some time ago that the speed of light is a hard upper limit on how fast you can communicate; there comes a point when the only thing you can do is move the content and computation closer! That’s why we put data centers in more than 275 cities all across the world: to give you what you’re looking for quickly!

***Cloudflare also provides security by protecting Internet properties from malicious activity like***[***DDoS attacks***](https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/)***, malicious bots, and other nefarious intrusions.***

And allows website owners to easily insert applications into their websites without needing to be a developer.

If you’re a developer, we allow you to run Javascript code on our powerful edge network, so that you can get as close to a user as possible. This eliminates delays, and improves the experience for users like you!

We provide security and performance for millions of Internet properties and offer great functionality such as [SSL](https://www.cloudflare.com/learning/security/glossary/what-is-ssl/) and [content distribution](https://www.cloudflare.com/cdn/) to every website on our network.

Our services run silently in the background, keeping many of the websites and services you depend on up and running.

Your Internet provider, and anyone else listening in on the Internet, can see every site you visit and every app you use — even if their content is encrypted. Cloudflare offers a [free DNS service called 1.1.1.1](https://www.cloudflare.com/learning/dns/what-is-1.1.1.1/) that you can use on any device. Cloudflare’s 1.1.1.1 protects your data from being analysed or used for targeting you with ads.