Content Delivery Network

Asad Zaman (p180034)

March 26, 2021

1 Introduction

A Content Delivery Network (CDN) is a system of geographically distributed servers that work together to provide fast delivery of Internet content. It's designed to minimize latency in loading web pages by reducing the physical distance between the server and the user. A CDN allows for a quick transfer of assets needed to load content such as HTML pages, javascript files, stylesheets, images, and videos. A well-configured CDN can also help protect against common malicious attacks such as Distributed Denial of Service (DDoS) attacks. Over half of all internet traffic is served by CDNs.

2 Working

To minimize distance between visitors and the website's server, a CDN stores a cached version of its content in multiple geographic locations known as the points of presence (PoP). Each PoP contains caching servers designed to deliver content to visitors within its proximity.

For example, a visitor in the United States wishing to view content that originates from a UK-based server will have to deal with slow loading times if the request has to travel across the Atlantic Ocean. To eliminate the latency, a CDN will store the content in a local United States PoP.

3 Case Study: Cloudflare

3.1 What is Cloudflare?

CloudFlare is a CDN(Content Delivery Network) which protects website from attacker. Does it host website on their webserver? No, They don't host website but in simple way we can say that it builds a wall between the Host and the visitor of that specific website.

3.2 Working

Cloudflare is designed to accelerate and secure any website. Our system works somewhat like a Content Delivery Network (CDN), but is designed to be much easier to setup and configure.

To explain how the system works, imagine you have a website (essayyzed.net) and it's running a web server with the IP address of 1.1.1.1. Before Cloudflare, if someone typed your website's

domain (allen.com) into their browser, the first thing that visitor's computer would do is send a query to the DNS system and get back your web server's IP address (1.1.1.1).

In order to make Cloudflare easy to set up, we take advantage of how this basic function of the Internet works. Rather than having you add hardware, install software, or change your code, we have you designate two Cloudflare nameservers as the authoritative nameservers for your domain (e.g., essayyzed.ns.cloudflare.com and nu.ns.cloudflare.com).

Designating Cloudflare as your authoritative nameservers doesn't change anything about your website. Your registrar remains your registrar, your hosting provider remains your hosting provider, and so on. However, because we are your authoritative nameserver, we can begin cleaning and accelerating your web traffic.

To make this happen we use a network routing technology called Anycast (and some other fancy tricks) to route initial DNS lookups for your domain to a Cloudflare data center closest to the visitor. We have data centers around the world and we're growing every month. The data center that receives the request returns an answer in the form of an IP address (e.g., 99.99.99.99), which directs all the visitor's subsequent requests to the best data center for them.

After a visitor's browser has done the initial DNS lookup, it begins making requests to retrieve the actual content of a website. These requests are directed to the IP address that was returned from the DNS lookup. Before Cloudflare, that would have been 1.1.1.1, with Cloudflare as the authoritative nameserver that would be 99.99.99.99 (or some other address depending on what Cloudflare data center is closest to the user). Cloudflare's edge servers running on that IP address receive the request and perform analysis on it. We scan to see if the visitor appears to be a threat based a number of characteristics including the visitor's IP address, what resource they are requesting, what payload they are posting, how frequently they're making requests, etc.