How Cloudflare erroneously throttled a customer's web traffic

02/07/2023

 Jeremy Hartman  Jérôme Fleury

4 min read

This post is also available in 简体中文, 繁體中文.

Over the years when Cloudflare has had an outage that affected our customers we have very quickly blogged about what happened, why, and what we are doing to address the causes of the outage. Today's post is a little different. It's about a

single customer's website not working correctly because of incorrect action taken by Cloudflare.

Although the customer was not in any way banned from Cloudflare, or lost acc to their account, their website didn't work. And it didn't work because Cloudflare applied a bandwidth throttle between us and their origin server. The effect was that the website was unusable.

Because of this unusual throttle there was some internal confusion for our customer support team about what had happened. They, incorrectly, believed that the customer had been limited because of a breach of section 2.8 of our Self-Serve Subscription Agreement which prohibits use of our self-service CDN to serve excessive non-HTML content, such as images and video, without a paid plan that includes those services (this is, for example, designed to prevent someone building an image-hosting service on Cloudflare and consuming a huge amount of bandwidth; for that sort of use case we have paid image and video plans).

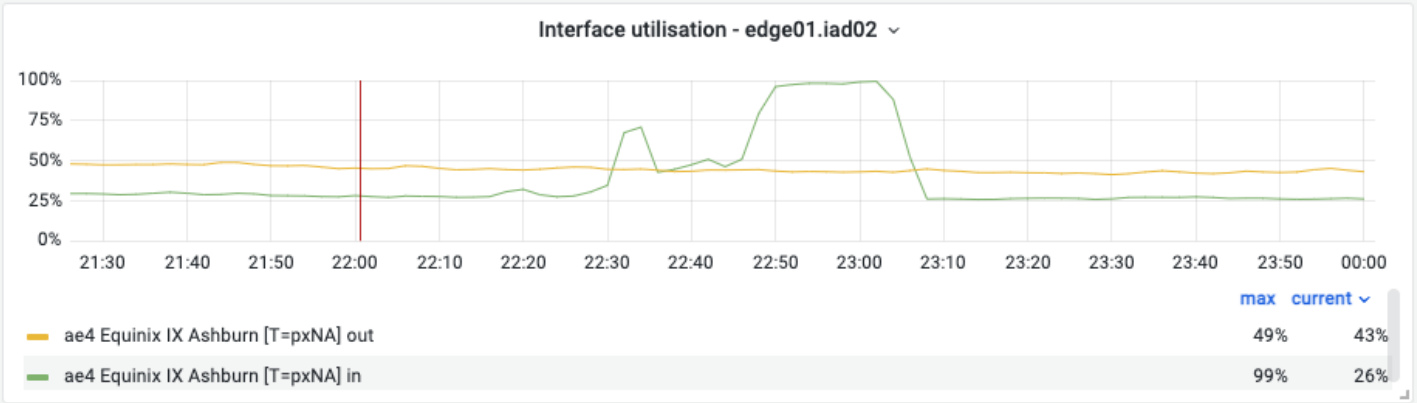
However, this customer wasn't breaking section 2.8, and they were both a paying customer and a paying customer of Cloudflare Workers through which the throttled traffic was passing. This throttle should not have happened. In addition, there is and was no need for the customer to upgrade to some other plan level.

This incident has set off a number of workstreams inside Cloudflare to ensure better communication between teams, prevent such an incident happening, and to ensure that communications between Cloudflare and our customers are much clearer.

Before we explain our own mistake and how it came to be, we'd like to apologize to the customer. We realize the serious impact this had, and how we fell short of expectations. In this blog post, we want to explain what happened, and more importantly what we're going to change to make sure it does not happen again.

Background

On February 2, an on-call network engineer received an alert for a congesting interface with Equinix IX in our Ashburn data center. While this is not an unusual alert, this one stood out for two reasons. First, it was the second day in a row that it happened, and second, the congestion was due to a sudden and extreme spike of traffic.



The engineer in charge identified the customer's domain, tardis.dev, as being responsible for this sudden spike of traffic between Cloudflare and their origin network, a storage provider. Because this congestion happens on a physical interface connected to external peers, there was an immediate impact to many of our customers and peers. A port congestion like this one typically incurs packet loss, slow throughput and higher than usual latency. While we have automatic mitigation in place for congesting interfaces, in this case the mitigation was unable to resolve the impact completely.

The traffic from this customer went suddenly from an average of 1,500 requests per second, and a 0.5 MB payload per request, to 3,000 requests per second (2x) and more than 12 MB payload per request (25x).

The congestion happened between Cloudflare and the origin network. Caching did not happen because the requests were all unique URLs going to the origin,

and therefore we had no ability to serve from cache.

A Cloudflare engineer decided to apply a throttling mechanism to prevent the zone from pulling so much traffic from their origin. Let's be very clear this action: Cloudflare does not have an established process to throttle customers that consume large amounts of bandwidth, and does not intend to have one. This remediation was a mistake, it was not sanctioned, and we deeply regret it.

We lifted the throttle through internal escalation 12 hours and 53 minutes after having set it up.

What's next

To make sure a similar incident does not happen, we are establishing clear rules to mitigate issues like this one. Any action taken against a customer domain, paying or not, will require multiple levels of approval and clear communication to the customer. Our tooling will be improved to reflect this. We have many ways of traffic shaping in situations where a huge spike of traffic affects a link and could have applied a different mitigation in this instance.

We are in the process of rewriting our terms of service to better reflect the type of services that our customers deliver on our platform today. We are also committed to explaining to our users in plain language what is permitted under self-service plans. As a developer-first company with transparency as one of its core principles, we know we can do better here. We will follow up with a blog post dedicated to these changes later.

Once again, we apologize to the customer for this action and for the confusion it created for other Cloudflare customers.

DDoS attacks, keep *hackers at bay*, and can help you on *your journey to Zero Trust*.

Visit 1.1.1.1 from any device to get started with our free app that makes your Internet faster and safer.

To learn more about our mission to help build a better Internet, start here. If you're looking for a new career direction, check out our open positions.

Discuss on X

Discuss on Hacker News

Discuss on Reddit

Follow on X

Jérôme Fleury | @Jerome_UZ
Cloudflare | @cloudflare

RELATED POSTS

August 29, 2023 8:00 AM

Cloudflare's tenant platform in action: Meter deploys DNS filtering at scale

Today, we're excited to showcase Meter, a provider of Internet infrastructure, is leveraging the Tenant API integration for DNS filtering to help their clients enforce acceptable Internet use policies...

By Mythili Prabhu, Ankur Aggarwal, Sean Rose (Guest author)

DNS Filtering, Customers

June 23, 2023 8:00 AM

How we scaled and protected Eurovision 2023 voting with Pages and Turnstile

More than 162 million fans tuned in to the 2023 Eurovision Song Contest, the first year that non-participating countries could also vote. Cloudflare helped scale and protect the voting application based.io, built by once.net using our rapid DNS infrastructure, CDN, Cloudflare Pages and Turnstile...

By Dirk-Jan van Helmond, Michiel Appelman, Jim de Beer (Guest Author)

Speed Week, Cloudflare Pages, Turnstile, Customers, Customer Success, DNS, Speed, Reliability

May 16, 2023 8:00 AM

Goodbye, section 2.8 and hello to Cloudflare's new terms of service

We're excited to announce new updates that will modernize our terms of service and hopefully cut down on customer confusion and frustration....

By Eugene Kim

Developer Week, Developers, Legal, Transparency, Customers

May 20, 2021 8:00 AM

Improving your monitoring setup by integrating Cloudflare's analytics data into Prometheus and Grafana

Here at Labyrinth Labs, we put great emphasis on monitoring. Having a working monitoring setup is a critical part of the work we do for our clients. Improving your monitoring setup by integrating Cloudflare's analytics data into Prometheus and Grafana...

By Martin Hauskrecht

Analytics, Customers, Prometheus, Grafana, Monitoring