CloudFlare Works with GlobalSign to Make SSL Faster Across the Web

01 Nov 2012 by Matthew Prince.

Earlier this week we announced how CloudFlare enabled OCSP stapling (http://b og.c oudf are.com/ocsp stap ng how c oudf are just made ss 30) in order to improve our customers' SSL performance. OCSP stapling is awesome and improves SSL performance by as much as 30%. However, it is limited to browsers that support OCSP stapling and only benefits CloudFlare's customers. So, until every browser vendor updates to support OCSP stapling and until every website uses CloudFlare, we wanted to see if we could do something else to improve SSL performance across the web.

GlobalSign Partnership

CloudFlare has worked with GlobalSign since we first launched in September 2010. Prior to that we surveyed nearly every certificate authority in an effort to find one that was forward thinking enough to support what we needed. GlobalSign has been a terrific partner and is shaking up what has been a commodity industry.

Several months ago, GlobalSign approached us to talk about SSL performance. Their goal was simple: become the fastest SSL provider on the Internet. As I've written about before, whenever you visit a websitover a HTTPS connection your browser has to perform a check to see if the certificate has been revoked (http://b og.c oudf are.com/how c oudf are s mak ng ss fast) . Depending on your browser, these checks are either over the CRL (Certificate Revocation List) or OCSP (Online Certificate Status Protocol) protocol. In either case, they require a request be sent back to the certificate authority and to get a response before content is downloaded. In other words, CRL and OCSP requests inherently slow down HTTPS performance.

The amount that these checks slow down performance varies depending on the certificate authority. On average, across the industry, a typical OCSP or CRL response time can be 500ms. That's half a second. In other words, every time you visit a site over HTTPS, you waste half a second waiting for the SSL check to complete. Talking with GlobalSign we realized we could do something about that.

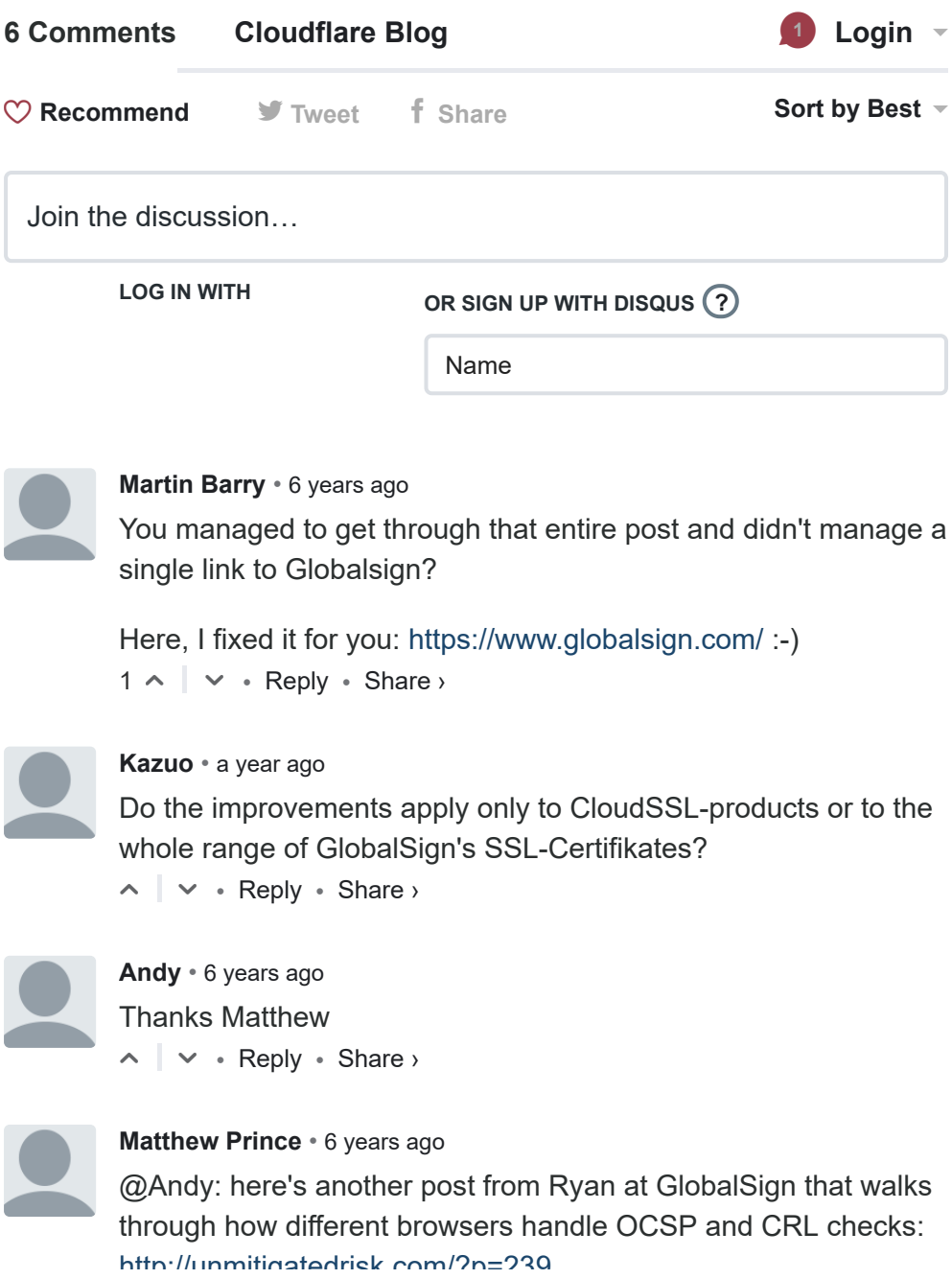
Now Saving 1.5 Years Worth of Time a Day

This morning we officially announced our work with GlobalSign to make their CRL and OCSP requests the fastest on the Internet. GlobalSign's SSL checks (OCSP and CRL GET and POST requests) are now served from our cache across CloudFlare's global infrastructure. The results have been awesome. The requests that previously averaging around 500ms are now under 100ms (http://unm t gatedr sk.com/?p=147) . At GlobalSign's scale, that means we're now saving the web about a *year and a half of time every day* that people would have otherwise spent waiting for web pages to load. That's crazy.

This improvement accrues to sites using GlobalSign SSL certificates, regardless of whether the sites themselves are running on CloudFlare's network. Getting more sites using SSL is critical for increasing web security and promoting new performance protocols like SPDY. If you are choosing a CA, typically a commodity decision, now there's a good reason to pick GlobalSign over the other choices: they will ensure your site is as fast as

possible over HTTPS. Put simply, GlobalSign is now the fastest certificate authority in the world, and nearly 3x as fast as Symantec/Verisign (http://unm t gatedr sk.com/?p=147) .

CloudFlare's mission is to power a faster, safer Internet so working with GlobalSign to make SSL as fast as possible has been a perfect fit. Our hope is that other certificate authorities will follow GlobalSign's lead and spend the time to optimize their SSL checks for optimal performance. As an added bonus, we've also helped GlobalSign be the first certificate authority to have their SSL checks be available over IPv6. This is all part of our efforts to help build a better Internet. As we like to tweet: #savetheweb (https://tw tter.com/search/rea t me?q=%23savetheweb) .



http://unmitigatedrisk.com/?p=239

Reply • Share ›

Matthew Prince • 6 years ago

@Andy: Here's a link about how Google's Chrome is handling revocations. It's not exactly correct that they're not doing checks anymore, as this post explains, they're just doing it in their own, proprietary way: http://unmitigatedrisk.com/?p=236

Reply • Share ›

Andy • 6 years ago

Is there a source where one can find out how the top 5 browsers handler revocation checks? Chrome has stopped performing the check altogether and others seem to be doing a soft check. http://www.darkreading.com/authentication/167901072/security/n

Reply • Share ›

ALSO ON **CLOUDFLARE BLOG**

Cloudflare Peering Portal - Beta

7 comments • 17 days ago

Jerome — We have to validate ownership of each ASN. If you haven't submitted a peeringDB

Lagos, Nigeria - Cloudflare's 155th city

7 comments • 9 days ago

eastdakota — I think you'll be happy with what's to come in both Pakistan and India.

A Tour Inside Cloudflare's G9 Servers

18 comments • a month ago

eastdakota — We've been

Mapping Factorio with Leaflet

2 comments • a month ago

Moscato — Why do you say backblaze in this context?