FLYWHEEL

Best Practices for Security and Speed - Updated Q1 2021

This document covers nearly every feature on Cloudflare. Some of these features may only be available for Pro, Business, or Enterprise plans and not the free offering. Nevertheless, it gives an overall view of the best practice settings that our customers using Cloudflare should be using to keep their sites as secure and fast as possible.

DNS

If on a Business or Enterprise plan, enable custom nameservers. This will aid in obfuscating that you are using Cloudflare and it gives a more white-label feel.

If the domain name registrar supports it, enable DNSSEC. This will prevent malicious actors from commandeering DNS requests via a man-in-the-middle attack or other forgeries.

SSL

- If the site has any SSL installed on Flywheel (Simple or BYO), ensure the SSL setting in Cloudflare is set to Full. Using Full (Strict) may not work, but if explicitly needed send us a support ticket to see if it's possible. Flexible should not be used if there's a certificate installed on Flywheel (it will cause redirect loop error)
- Flexible works great for securing secondary domains, but it should not be used on a domain covered by Flywheel's Simple or BYO SSL
- Enable Always use HTTPS (This enforces HTTPS from the Cloudflare edge which is more quick to initiate the redirect but if issues arise may need to be temporarily disable to troubleshoot redirection or Simple SSL validation errors.)
- If planning to always use HTTPS, Enable HSTS with 12 month age, include subdomains on, and preload on. HSTS will allow select browsers to index the site as HTTPS-only so tha

- t it loads the site more quickly and there will not be a 301 redirect from HTTP to HTTPS
- Minimum TLS Version can stay at TLS 1.0 (default)
- Enable Opportunistic Encryption
- Keep Onion Routing enabled (if you'd like users of TOR to access your site)
- Enable TLS 1.3 support
- Enable Automatic HTTPS Rewrites
- Enable Certificate Transparency Monitoring and enter the desired email to be notified. This will help ensure you are notified if someone else is maliciously attempting to have an SSL certificate issued for your domain.

Firewall

- Ensure that the Cloudflare managed rulesets for Misc, PHP, Specials, and WordPress are enabled. **Additionally, click on the rule name in order to enable further rules and change the "mode" from challenge to block, etc.** (tip: consult with a security expert to ensure the correct rules for your application-type are enabled)
- Ensure all OWASP rules are enabled, except the Joomla and PHPBB rules
- Create custom firewall rules to block and/or challenge based on Cloudflare's Threat Score as outlined here: https://community.cloudflare.com/t/threat-score/37874
- Create custom firewall rules (see how here: https://blog.cloudflare.com/announcing-firewall-rules/) to block and/or challenge known malicious user agents. Here's a list of ones that may be considered worthy of blocking: https://pastebin.com/Fgn5e9AH
- If you want to block traffic from countries that aren't a part of the target market, you can also use custom firewall rules. Check out this further guide on blocking countries with Cloudflare here.
- Enable rate-limiting. This will help stop most DDoS, Brute Force, and other flood attacks. You can read more on this here: https://www.cloudflare.com/rate-limiting/ (**Pro tip:** if using rate-limiting *and* LogFlare, be sure to whitelist LogFlare's IPs)
- Block XMLRPC from the Cloudflare edge. https://www.sertmedia.com/blocking-xmlrpc-access-in-wordpress-using-cloudflare/
- Click Settings on Firewall tab and ensure the "Bot Fight Mode" is enabled

Access

Cloudflare Access lets you lockdown specific sections of your site. This is especially useful for locking down WP Admin. Cloudflare Access will act as a gateway to WP Admin (or any other page selected) and require 2FA. The other benefit besides the 2FA functionality is Access will

prevent Brute Force attacks. Depending on the number of users who will be using Access, the feature is free.

Speed

- Enable Image Resizing. It allows on the fly resizing requests of 100,000 on the Business plan or up to 10 million requests on Enterprise plan. This lets you easily set specific directives for max image size, resolution, etc. By enabling the image resizing parameters, it ensures all images are of equal size and there aren't any too large that will bloat the site. Read more on setting that up here: https://developers.cloudflare.com/images/about/
- Enable Polish with Lossy compression. Enable WebP support
- Enable Auto Minify for each static asset type
- Enable Brotli
- Enable Automatic Platform Optimization for WordPress and install plugin
- Enable Enhanced HTTP/2 Prioritization
- Enable Mirage to help users with slower mobile connections load images more quickly
- Enable Rocket Loader. This feature will significantly improve your site's paint time. However, test your site after enabling to ensure that all Javascript elements are loading and the site functions normally
- Railgun, while a uniquely cool feature from Cloudflare, we're currently not supporting it at this time.
- Add prefetched URLs. You can use this to prefetch static assets you know will be loading regularly such as JS, CSS, logos, etc. (only available on Enterprise plan)

Caching

- Keep caching level at standard (unless needing to bypass query strings)
- Set browser cache to 1 month, or lower/more as needed
- Enable Always Online
- Ensure Query String Sort is enabled (Enterprise plan only)
- Enable Child Sexual Abuse Material (CSAM) Scanning Tool - useful if content is user-generated. Helps you fight against illegal content.

Workers

Workers let you run Javascript from the Cloudflare edge (i.e. across their global network of over 193 data centers). There is a small fee for using a Worker. However, the benefit far outweighs the cost. With a Worker, you can cache your site's HTML at the edge. This will significantly

improve site performance. There is even an accompanying plugin to install that will assist with purging edge cache should you publish, update, or make other changes to the site. I highly recommend taking a look at setting it up here: https://github.com/cloudflare/worker-examples/tree/master/examples/edge-cache-html

NOTE - With the introduction of "Automatic Platform Optimization for WordPress" feature, as listed in the Speed section, the Workers example listed above is no longer relevant with regard to edge caching. However, Workers are still a unique way to store Javascript at the edge and might be useful depending on your application's needs.

Page Rules

Using Page Rules will let you take advantage of handling redirects at the DNS-level. This will allow redirects to occur much, much faster than if we were to place the redirects via NGINX. Page Rules will also let you manage security, cache, and more for specific URLs you list.

In addition, you can use a Page Rule to also cache HTML to the edge. This is similar to the functionality of the Worker feature above. The only difference is that the Page Rule for "cache everything" will not purge should a post be published or updated. It will also not natively bypass cache for WooCommerce store pages. Instead, you would need to set specific bypass on cookie rules as detailed here: https://support.cloudflare.com/hc/en-us/articles/236166048-Caching-Static-HTML-with-WordPress-WooCommerce

Ensure WP Admin is bypassed from Cloudflare cache. You can likely keep the security settings, but ensure caching and other settings are disabled to prevent any complications. https://support.cloudflare.com/hc/en-us/articles/200169526-Disabling-Cloudflare-features-on-admin-pages-for-content-management-systems-like-WordPress

Network

- Ensure HTTP/2 support is enabled
- Enable HTTP/3 with QUIC
- Enable 0-RTT Connection Resumption
- Ensure IPv6 Compatibility is enabled
- If WebSockets are needed for your site, enable the option
- Enable gRPC if you use gRPC API endpoints

- Set Pseudo IPv4 to “add header”
- Ensure that IP Geolocation is enabled

Traffic

Enable Argo. This premium feature will ensure traffic is routed more quickly as it's prioritized across Cloudflare’s network, therefore, improving the load time of your site.

Stream

If you intend to host videos, it is strongly suggested to not use YouTube/Vimeo, but instead, use Cloudflare Stream. The Stream service lets you host your video across the Cloudflare network and then easily embed it in your posts/pages. Our parent company, WP Engine, teamed up with Cloudflare to create a simple plugin that will let you more easily embed any videos added to Cloudflare Stream. Check it out here: https://wpengine.com/blog/wp-engine-launches-cloudflare-stream-video-plugin-for-wordpress/

Apps

Using Google Analytics? Don’t host it on your site. Instead, enable Google Analytics from Cloudflare Apps section and have the GA code hosted on the Cloudflare edge.

Want a granular way of viewing your logs? Enable the free, open-source App called LogFlare. Read more about it here: https://logflare.app/

Scrape Shield

Ensure that every option in this section is enabled. The hot-linking protection is by far the most important, as it will prevent unauthenticated users from eating up your bandwidth by directly linking to your images on their own sites.

Caveat - This may break Open Graph media, when items are shared to social networking platforms such as Facebook, Twitter, etc.