Notes for DNCSEC from CloudFlare

Secure DNS or DNSSEC

DNSSEC, or DNS Security, is a newer protocol that expands upon the early DNS protocol. Still using port 53, DNSSEC only uses TCP due to the MTU being too large for UDP, unlike plain DNS. It is used to prevent or hinder some common network attacks such as DNS Hijacking, DNS Poisoning, and Man-in-the-Middle attacks. Most of the DNS attacks exploit unsecured DNS protocol which allows threat actors to impersonate valid querists by exploiting vulnerabilities in name resolution. DNS attacks are especially dangerous because they are easily exacerbated by the normal internet practices of normal users, and are very hard to users to detect. DNSSEC (DNS Security Extensions) uses digital signatures on the transmitted data to ensure integrity and non-repudiation, and to prevent DNS forgeries. Hierarchical digital signatures are present at all layers of the DNS protocol in DNSSEC. DNSSEC is backwards compatible, such that traditional, non-secure DNS lookups still resolve correctly. DNSSEC requires TLS or SSL.

Additionally, DNS Server redundancy, A.K.A. Anycast Routing a CloudFlare-specific from of load balancing, can prevent DNS-based DDoS attacks. CloudFlare touts the lowest DNS query speed, as well as the fastest DNS propagation, and as the only one specifically mentioned by name in Michael’s outline, it will be the one that I will initially test.

How it works

CloudFlare’s DNSSEC adds an authentication layer to DNS and guarantees that querists reach the website they intended to, supplanting Man-in-the-middle attacks and DNS poisoning. DNS is a very early protocol and is fundamentally insecure. CloudFlare’s DNSSEC claims to secure the infrastructure using zone enumeration, in addition to certificate infrastructure, and a handy set of additional internet tools.

According to Rob and Ryan, most of our client’s registrars are GoDaddy or NameCheap. Both of these services will work with CloudFlare’s DNSSEC. Network Solutions will probably work as well but there is less certain documentation on that, and it is not explicitly stated as being one of the suggested registrars. Using CloudFlare’s DNS services with a different registrar requires that the CloudFlare user obtains the DS Record from CloudFlare’s control panel, and manually add that to the registrar control panel. The following guide features a table that illustrates the procedure for each of the most popular registrars: <https://support.cloudflare.com/hc/en-us/articles/360006660072#nodnssec>

CloudFlare uses a dashboard/control panel over HTTPS. Their preferred encryption cipher is the asymmetric Algorithm 13, which features elliptical curve cryptography (low processing requirements), zone signing, and digital signatures. This is the same encryption protocol that is used by Bitcoin to ensure confidentiality, integrity, and non-repudiation.

According to DNSSECready.net, https://sets.solar will be fine to implement DNSSEC since the .solar top-level domain (TLD) is signed and validated. This will definitely prohibit any domain with more unusual TLDs like .vi or .tel. I could think of no other clients that has non-standard TLDs.

DNSSEC adds additional record types, including RRSIG, DNSKEY, DS, NSEC(3), and CDS or CDNSKEY. The most important of these for troubleshooting purposed will be the DS record, which contains a hash of the DNSKEY record and must be manually added to registrar’s records. DNSSEC also creates RRsets, which are collections of records with the same type (A, CNAME, MX, etc.), that are grouped into resource record sets, which are then digitally signed.

Whenever a DNSSEC resolver requests a particular record type (like AAAA), the name server will return the record in addition to a corresponding RSIG record, which contains a cryptographical digital signature.

DNSSEC is to DNS what HTTPS is to the internet. DNSSEC adds additional layers of security by authenticating and signing. DNSSEC does not *encrypt* DNS queries, unlike HTTPS. Instead it offers digital signatures so that MITM and DNS-poisoning attacks, and forgeries, redirects, and even DNS-hijacking are no longer threats.

Implementing CloudFlare DNSSEC is pretty straightforward. Once the service is started, DNSSEC can be added to any web property by enabling DNSSEC there and adding the DS record to the registrar. Going forward, it is also possible to use CloudFlare as a registrar, such that, conveniently, DNSSEC is included.

Testing

I have enrolled for the free version of DNSSEC through CloudFlare, and the process begins with entering the site you own, then allowing CloudFlare to query your site’s existing DNS records, later importing them into CloudFlare’s database. Then the nameservers will need to be changed to CloudFlare’s nameservers, where they tout a <5m DNS propagation. The free version I selected includes global content delivery network (CDN) which provides cached content, high availability, increased security against DDoS attacks. It also includes optional custom SSL certificates for your site. The “Business” pricing model is $200 per month, and includes Web Application Firewalls with custom CloudFlare rulesets, TLS-only-mode, custom SSL certificates, and image/mobile-browser optimizations. The Enterprise level required a call to determine pricing, and features the best support, with 24/7 coverage by chat, email, or phone, in addition to access to raw request logs, and 100% uptime guarantee with a very generous reimbursement for SLA violations.

CloudFlare’s auto lookup got every record for my grandmother’s website, <https://www.horwitzstudio.com>, hosted on WordPress. Despite WordPress’s assertion that using non-WordPress nameservers would cause “some WordPress features to fail to load”, I saw no impact in performance or availability. WordPress isn’t known for being the most lightweight and adaptable service, and even still it seemed to work fine.

The <5m propagation was nullified by the admission that it may take up to 24 hours for the registrar to publish the changes. At 12:15pm on Thursday the 9th, I made the change, and I ran a constant ping on my Linux machine to see if the IP address change was detectable. I wrote a short recuring script that runs a traceroute every 60 seconds and pipes the output into a text file. The script and the output of that text file over a 12 hour period are available on my Github: <https://github.com/bcornw2/>

Features

CloudFlare offers a service called “I’m Under Attack Mode!”, which creates and interstitial page with a Javascript puzzle (like a Captcha) to negate DDoS attacks. The use of this feature was very easy (literally a button on the top of the dashboard that can be turned on in seconds), and even though my grandmother’s piano-lesson website, which gets about 4 unique visitors a month, wasn’t really under attack, it would have been safe if it was.

CloudFlare also offers interesting “page rules” that can be configured for each website. My favorite is mandating HTTPS for all site visitors. It also allows Geolocation and Minify plugins and about 25 other settings with entire sub-rule-sets beyond that. Paired with Email Address Obfuscation for bots, CloudFlare appears to be a good move for anyone aiming for defense in depth for their internet properties.

The Access tool is also interesting: it will segment off certain parts of your web property and allow only authenticated users to reach that area. This could be useful for an external site having private information for employees while having both parties go through the main site. When an unauthorized user tries to access privileged info, he will be unable to reach those resources, where a credential-required information would be. This ould have some interesting applications as per the client/customer/visitor versions of privileged vs non-privileged information.

The caching feature is also a nice addition, especially in my free-only version. Caching, bandwidth baselining, DNS request measurements, and the graphical site traffic management console are all very useful features that are definitely not included in even my premium WordPress or SiteGround subscriptions. While my free version did not have access to the CloudFlare DNSSEC service, or the custom nameservers, as it would with Business or Enterprise, it was still an enjoyable experience and I will probably keep my free version active on my site.

Use and Experience

The dashboard is very user-friendly and has a professional and clean GUI. The categories were itemized about the top and were easy to navigate. Most of this may be cosmetic, but it is far better than the administrative console of some services like Mimecast’s administration page’s UI.

I think, most appropriately, CloudFlare’s “Country Block” service will benefit PPB, so I don’t have to spend all morning manually blocking various @mail.ru domains in their spam filter.

Take-aways

I did similar research on other DNSSEC and internet security services like UpCloud, CloudBric, Verisign, and others, but I’ve found CloudFlare to be at the forefront of this particular branch of information security, and to have the most complete and engaging toolset. The enterprise package also offers the best coverage for support, and according to some public opinion on various tech forums, CloudFlare also has the best quality of support.