**Cloudflare Settings Optimization**

**Updated 2024-11 – TLS 1.3 is replaced with TLS 1.2 to ensure that MTA-STS functions.**

1. Configure DMARC
   1. Under Email -> DMARC Management, Enable DMARC Management
      1. Additionally, The DMARC Aggregator Valimail (<https://app.valimail.com/>) is free for Office 365 Users, and works well as a secondary DMARC report Aggregator.
   2. Configure DKIM records for each server which should be allowed to send mail on behalf of the domain
   3. Configure SPF Record to include all servers which are allowed to send mail on behalf of the domain
2. On DNS -> Records Page for each domain
   1. Proxy only CNAME’s and A records which use HTTP or HTTPS. Other services will not work via proxied IP
      1. Shopify, Wix, and some other web vendors do no support this
   2. Configure CAA Records for Cloudflare, update the text in red below, this will receive reports on any failed cert issuance:
      1. @ 3600 CAA 0 issue "comodoca.com"
      2. @ 3600 CAA 0 issue "digicert.com; cansignhttpexchanges=yes"
      3. @ 3600 CAA 0 issue "letsencrypt.org"
      4. @ 3600 CAA 0 issue "pki.goog; cansignhttpexchanges=yes"
      5. @ 3600 CAA 0 issue "ssl.com"
      6. @ 3600 CAA 0 issuewild "comodoca.com"
      7. @ 3600 CAA 0 issuewild "digicert.com; cansignhttpexchanges=yes"
      8. @ 3600 CAA 0 issuewild "letsencrypt.org"
      9. @ 3600 CAA 0 issuewild "pki.goog; cansignhttpexchanges=yes"
      10. @ 3600 CAA 0 issuewild "ssl.com"
      11. @ 3600 CAA 0 iodef "mailto:alert@domain.com"
   3. Go to DNS -> Settings, click "Enable DNSSEC"
      1. Update DS record at registrar to complete enablement of DNSSEC
      2. For Domains within the Cloudflare Registrar, the DS record does not need to be updated manually.
      3. Verify this in 15 mins, via the link: <https://dnsviz.net/>
3. On SSL/TLS -> Edge Certificates Page for each domain
   1. Switch on “Always use HTTPS”
   2. Change HSTS Settings to below:
      1. Enable HSTS
      2. Max Age Header – 12 Months
      3. Include Subdomains: On
      4. Preload: On
      5. No-Sniff Header: On
   3. Minimum TLS Version: 1.2
   4. Opportunistic Encryption: On
   5. TLS1.3: On
   6. Automatic HTTPS Rewrites: On
   7. Certificate Transparency Monitoring: Off
4. On Security – Page Sheild Page, Enable Page Sheild
5. On Security – Bots Page
   1. Enable “Bot Fight Mode”
   2. Enable “Block AI Bots”
6. On Speed -> Optimizations Page
   1. Click “Enable All Available Settings”
   2. Go to “Protocol Optimization Page”
      1. Turn off 0-RTT Connection Resumption
7. On Caching -> Configuration Page
   1. Enable Crawler Hints
   2. Enable Always Online
8. On Caching – Tiered Cache Page
   1. Enable Smart Tiered Caching Topology
9. On Rules -> URL Normalization Page
   1. Enable Normalize incoming URLs
   2. Enable Normalize URLs to Origin
10. On Scrape Shield Page
    1. Enable Email Address Obfuscation
    2. Enable Hotlink Protection
11. Optional Items:
    1. On Caching -> Configuration Page
       1. Enable CSAM Scanning Tool using both lists
          1. Registration and Logon details for the NCMEC are required
    2. Transfer your eligible domains to Cloudflare, they are significantly cheaper than providers like Namecheap and GoDaddy ($10 per year for .com domains)
    3. Confirm the SSL Security Rating of the site at <https://www.ssllabs.com/ssltest/>