**Cloudflare Settings Optimization**

1. Additional Steps
   1. Configure DMARC
      1. The DMARC Aggregator Valimail (<https://app.valimail.com/>) is free for Office 365 Users
   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
   4. Confirm the SSL Security Rating of the site at <https://www.ssllabs.com/ssltest/>
      1. The Target is to achieve an A+ rating, which the settings below will achieve.
   5. If you are using WordPress, Install the Cloudflare WordPress add-on on your website, and allow it to auto-optimize
   6. Transfer your eligible domains to Cloudflare, they are significantly cheaper than providers like Namecheap and GoDaddy ($8 per year for .com domains)
2. On DNS 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
   2. Enable DNSSEC if available for your domain (be aware that some TLD’s and registrars do no support this yet)
   3. Configure CAA Records for Cloudflare, **as well as any other needed certificate providers**, Cloudflare settings below:   
      Graphical user interface, text, application

      Description automatically generated
3. On SSL/TLS Page for each domain
   1. Overview Page
      1. Set encryption mode to full
         1. This can be set to Full (strict), but a valid SSL cert must be installed on each proxied web server
            1. Alternatively, go to the Origin Server tab
            2. Create a certificate and install it on the web server (be advised that this cert cannot be used without cloudflare’s proxy
            3. Enable “Authenticated Origin Pulls”
      2. Switch on SSL/TLS Recommender
   2. On Edge Certificates Page
      1. Switch on “Always use HTTPS”
      2. Change HSTS Settings to below:
         1. Enable HSTS
         2. Max Age Header – 6 Month
         3. Include Subdomains: On
         4. Preload: On
         5. No-Sniff Header: On
      3. Minimum TLS Version: 1.2
         1. Setting this to TLS 1.3 will give an “A” rating instead, but is actually more secure, some older browsers may not work with this.
      4. Opportunistic Encryption: On
      5. TLS1.3: On
      6. Automatic HTTPS Rewrites: On
      7. Certificate Transparency Monitoring: On
   3. On Speed -> Optimizations Page
      1. Enable all 3 options in “Auto-Minify”
      2. Enable Brotli
      3. Enable Rocket Loader
   4. On Speed -> Browser Insights Page
      1. Click Configurations and Enable Browser Insights
   5. On Caching -> Configuration Page
      1. Enable CSAM Scanning Tool using both lists
         1. Registration and Logon details for the NCMEC are required
      2. Enable Always Online
   6. On Rules -> Settings Page
      1. Enable Normalize incoming URLs
      2. Enable Normalize URLs to Origin
   7. On Scrape Shield Page
      1. Enable Email Address Obfuscation
      2. Enable Server-side Excludes
      3. Enable Hotlink Protection