Basic Configuration

https://campus.barracuda.com/doc/97517690/

To configure the WAF-as-a-Service Content Delivery Network (CDN) for your application:

1. Set **Enable CDN** to **On** and click **Save**. You can remain on this screen while CDN activates or return later. A notification will pop up once all domains configured for your application are listed along with the associated TXT keys.
2. Configure your DNS by adding the TXT verification records to match these values. You can use the copy icons to capture the values to use when creating the records. Domains will automatically show as **Approved** once the records have propagated through the DNS system. How long this will take depends on the Time To Live established with each one.

   Skip this step if your DNS zone is hosted with WAF-as-a-Service. When the DNS zone is hosted with WAF-as-a-Service, the TXT records are automatically created for DNS and the CDN domain approval process gets completed.
3. Once all domains are **Approved**, you can set **Route traffic through CDN** to **On**. This begins the rollout of your application in the CDN network. Again, you do not need to remain on this page and you will be notified once rollout is finished.
4. Optional: By default, CDN will generate and manage certificates. However, you can provide your own certificate:
   1. Click the three dots in the **Action** column and select **HTTPS Settings**.
   2. In the pop-up window, select **Bring your own certificate (BYOC)** and enter your certificate and private key. Click **Add**.
5. Once rollout is complete, the **Enable CDN** setting will no longer be active and **Block traffic not sent through CDN** will become active. Enabling this will ensure all traffic goes through CDN and prevents other routes. However, doing so immediately could block legitimate traffic that is not routed via CDN yet, so it is a good practice to wait a few hours before blocking direct traffic.

Note: WAF-as-a-Service will automatically effect the following configuration changes once CDN is enabled:

- Increases the **Max Number of Headers** to a minimum of 40 in the Request Limits policy.
- If you have **CAPTCHA** enabled within your security policies, you need to change them to use **reCAPTCHA v2** or **reCAPTCHA v3** for them to work correctly in conjunction with the CDN (hint: DDoS and the Bot Protection components).