Endpoints

https://campus.barracuda.com/doc/76284376/

Barracuda WAF-as-a-Service accepts traffic for your application through *Endpoints*. An endpoint is a combination of an IP address and a TCP port. One application may have multiple endpoints. Each application must have at least one endpoint.

You might want an application to accept traffic on a number of endpoints if you want to accept:

- both HTTP (port 80) and HTTPS (port 443) traffic.
- traffic on a non-standard port, for example, port 8000 for HTTP traffic.

HTTPS Endpoints and SSL Certificates

When you configure an endpoint to use the HTTPS protocol, traffic between your users and Barracuda WAF-as-a-Service is encrypted with the SSL protocol. This requires WAF-as-a-Service to have an SSL certificate. By default, Barracuda uses the Let's Encrypt certificate authority to retrieve SSL certificates for your application. For security purposes, Let's Encrypt will only issue certificates if you have met the following two conditions:

- You modified the DNS records for *all of your domains* to point to the Barracuda-allocated endpoint address. Refer to Getting Started for information on how to modify the DNS records.
- You have an HTTP Endpoint on port 80. If you require different HTTP ports, you can add them as additional endpoints, but maintain the port 80 endpoint in addition.

Note

Note that if you change only some of your records, but not others, Barracuda will not be able to obtain a certificate for your endpoint. Users will see a certificate warning when they visit your application. To avoid this issue, be sure to change *all* DNS records associated with an endpoint *at the same time*.

The automated leasing of the certificate for the HTTPS endpoint will fail if the **Datacenter IPs** category is configured to be blocked in the **IP Address Geolocation** component. It is recommended to use your own certificate in the endpoint configuration if this category needs to be blocked from accessing the application.

Deployment Location

In general, performance improves when locate protection in a region that is close to your application servers. For the best performance, Barracuda WAF-as-a-Service automatically chooses the region nearest the IP address for your application servers as its deployment location. It then chooses the next closest location as a backup. Most deployments do not require any changes to these settings. If you have special circumstances, like data residency requirements, you might need to change this setting. For background information, refer to Understanding Deployment Locations. For information on changing a location, refer to Moving an Application to Another Location.

> The **North America and West Europe** location is now deprecated. Do not add new applications to that location. Move any existing applications within that location to a different location. Refer to Moving an Application to Another Location for details.

Deploying within a Container

If you are deploying your application within your own container, you must choose that container as the Deployment Location.

For details, refer to Deploying Your Own Containers.

IP Addressing

By default, applications will use an IP address shared with other applications. If your account is licensed with an Application Protection Premium plan (or your legacy license is configured with Isolated Mode), you can change to a dedicated IP address.

A dedicated IP address should only be necessary if you require one of these features:

- Processing traffic that does not include a *host* header matching one of the domain names you defined in your endpoints.
- Processing HTTP traffic on ports that are usually reserved for HTTPS, or vice versa.
- Adding TCP Proxy type endpoints.

It can take up to 8 hours to move to a dedicated IP address, but your application will experience no downtime during this change.

IP Ranges to Allow

See Restricting Direct Traffic to control which IPs are allowed to access your applications.

Provisioning Your Application

When you first add an application, it must be provisioned. During this process, which can take up to one hour, a message appears on the Endpoints page. To avoid potential downtime, wait until your application is fully provisioned before changing your DNS records.