Certificate Management

https://campus.barracuda.com/doc/19333369/

In an SSL transmission between a client and a server, the client requests a secure connection, and the server responds with a certificate, identifying the certificate authority (CA) and the server's public encryption key. This allows the client to verify the server identity. If satisfied with the authenticity of the server, the client sends a test transmission which can only be decrypted with the private key of the server. This transmission allows both parties to encrypt and decrypt the impending transaction. A server may refuse to communicate with clients that fail to provide a certificate for authentication.

The Barracuda Load Balancer ADC acts as a server on the front-end (Internet facing), receiving client requests. On the back end, the Barracuda Load Balancer ADC acts as a client to the web servers, forwarding safe requests to them. In each case, data can be secured using SSL, providing end-to-end secure data for requests and responses. Certificates can be obtained from a trusted CA or be self-signed.

The Barracuda Load Balancer supports SSL certificates in PKCS #12 and PEM formats. The certificates can be uploaded on the **BASIC > Certificates** page.

In this Section