Introduction to SSL Certificates

https://campus.barracuda.com/doc/4259855/

Overview

The Barracuda Web Application Firewall implements Secure Socket Layer (SSL) encryption using PKI objects, which encrypts transmitted data and allows authentication of sender and receiver. You can use SSL encryption between a client and the Barracuda Web Application Firewall, and/or between the Barracuda Web Application Firewall and web servers by creating or uploading certificates.

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. The certificate allows the client to verify the server identity.

The Barracuda Web Application Firewall acts as a server on the front end (Internet facing), receiving client requests. On the back end, the Barracuda Web Application Firewall acts as a client to the web servers, forwarding requests to them. In each case, you can use SSL to provide end-to-end secure data for requests and responses. The Barracuda Web Application Firewall allows certificates obtained from a trusted CA to be uploaded, or it can create a self-signed certificate to implement SSL.

Digital certificates created using the Barracuda Web Application Firewall are of the standard X.509 format and are considered self-signed.

SSL Implementation and Configuration

SSL for Client to Barracuda Web Application Firewall Transmissions

The Barracuda Web Application Firewall receives requests from clients on behalf of the back-end server. When a request is received from a client, the Barracuda Web Application Firewall acts as a server to the requesting client. It can be configured to provide a certificate (a self-signed certificate created on the unit, or a certificate issued by a trusted CA uploaded to the unit), which allows the client to authenticate the request transactions and send them in encrypted form.

For more information on how to generate self-signed certificates, or to upload trusted certificates, see How to Add an SSL Certificate.

To configure the Barracuda Web Application Firewall to use SSL in client communications, create an SSL-enabled service and refer to Configuring SSL between a Client and the Service for specific instructions on configuring SSL. Additionally, the Barracuda Web Application Firewall can be configured to require the client to provide a certificate for authentication, denying communication with clients who fail to do so.

SSL for Barracuda Web Application Firewall to Server Transmissions

The Barracuda Web Application Firewall also provides server-side encryption, and can provide a certificate to the servers for client authentication (the Barracuda Web Application Firewall acting as the client to the back-end servers). This protects services configured on the Barracuda Web Application Firewall. The client-server negotiations include the following:

- The Barracuda Web Application Firewall receives and verifies the server’s certificate.
- The Barracuda Web Application Firewall may provide a certificate in return, if client authentication is required by the back-end server.

The SSL handshake allows the server and the Barracuda Web Application Firewall to authenticate each other. Once mutually authenticated, both use keys for encryption, decryption, and tamper detection during the SSL sessions.

To configure the Barracuda Web Application Firewall to use SSL in server communication, go to **BASIC > Services** and **Add** a server for the respective service**.** Then, configure the Barracuda Web Application Firewall to validate the server certificate and, optionally, to present a client certificate. See Configuring Server Settings. For information on client certificates, see Allowing or Denying Client Certificates.

Related Article:

- Barracuda Web Application Firewall Integration with Venafi