How to Add an SSL Certificate

https://campus.barracuda.com/doc/4259930/

Overview

A signed certificate is a digital identity document that enables both server and client to authenticate each other. Certificates are used with HTTPS protocol to encrypt secure information transmitted over the internet. A certificate can be generated or procured from a third party Certificate Authority (CA). Generated certificates can be self-signed or signed by a trusted third-party CA. A certificate contains information such as user name, expiration date, a unique serial number assigned to the certificate by a trusted CA, the public key, and the name of the CA that issued the certificate.

Certificate Components

Key Pair

The Barracuda Web Application Firewall implements an asymmetric methodology for encryption, where two related keys are used in combination. A key pair consists of a public key and a private key which work together, with one of the key pair encrypting messages, and the other decrypting encrypted messages.

Exposure of the public key does not endanger the secure transactions because the private key cannot be derived from it.

Distinguished Name (DN)

The Distinguished Name (DN) in the certificate uniquely identifies the public key owner who issues the certificate.

Token

A token is a cryptographic item used for secure storage and transfer of private interface and certificate. Currently, the Barracuda Web Application Firewall supports only the PKCS #12-type token. The PKCS #12 token can be loaded onto the Barracuda Web Application Firewall from a remote system or saved from the Barracuda Web Application Firewall onto a remote system.

CA Certificate

A trusted certificate is a third-party certificate issued by a Certificate Authority (CA) which can be

uploaded and saved on the Barracuda Web Application Firewall. This certificate can be added to a certificate chain, where it is used for encryption and authentication. Browsers requiring certificates from a CA will require the procurement and upload of the certificate before communication between a client and a server can be established.

The Certificates managed by the Barracuda Web Application Firewall:

- Self-signed Certificates
- Trusted Certificates

Self-signed Certificate

A self-signed certificate (also called user certificate) can be generated by the Barracuda Web Application Firewall to provide strong encryption without the cost of purchasing a certificate from a trusted certificate authority (CA). However, web browsers cannot verify the authenticity of the certificate and therefore display a warning every time a user accesses the administration interface. Because of this, self-signed certificates are ideal for test purposes, and may not be desirable as a production solution.

Trusted Certificate

Trusted certificates, issued by trusted Certificate Authorities (CA), are usually recognized by web browsers and no additional configuration is required.

Creating a Self-signed SSL Certificate

A self-signed X.509 digital certificate can be created by the Barracuda Web Application Firewall. The X.509 certificate type is one of the most common, and the International Telecommunication Union (ITU) recommends it, but it is not the industry standard for certificates. So an X.509 certificate generated by the Barracuda Web Application Firewall may or may not be accepted by clients or web servers.

To create a self-signed SSL certificate:

1. Go to the **BASIC > Certificates** page, and click **Create Certificate** in the **Certificate Generation** section.
2. Follow the displayed instructions to fill in all fields.
3. Click **Generate Certificate**.

Signed Certificate

A self-signed certificate signed by a trusted Certificate Authority (CA) is known as a Signed Certificate. The generated certificates are stored in the **Saved Certificates** section. A Certificate Signing Request (CSR) is created each time you generate a certificate using the Barracuda Web Application

Firewall. It contains information such as organization name, domain name, locality, country and the public key. To convert a self-signed certificate to a signed certificate, download the CSR file and send it to a trusted third party CA such as VeriSign or Thawte for signing. A CA administrator verifies the CSR, signs the request, and returns a signed certificate to be used for SSL based Services.

Steps to Download a CSR:

1. Go to the **BASIC > Certificates** page.
2. In the **Saved Certificates** section, identify the certificate that needs to be signed by a third party trusted CA.
3. Click **CSR** under the **Download** option. A pop-up window appears. Select **Save File** to save the file to the location you desire. A CSR file is saved with the extension .csr.
4. You can send this CSR file to a trusted Certificate Authority (CA) for signing. A CA verifies the CSR and returns a signed certificate SSL based Services can use.

Once the CSR is signed and returned, the certificate file is replaced by the new certificate. Extract the key and upload the signed certificate on the Barracuda Web Application Firewall.

Steps to Extract the Key from a Certificate:

1. Click **Certificate** under the **Download** option. The **Save Token** pop-up window appears.
2. Enter the pass phrase in the **Encryption Password** field and click **Save**. The certificate gets exported as a PKCS #12 token.
3. Extract the private key from the PKCS #12 token using the same pass phrase. The openssl command used to extract the key is: "*openssl pkcs12 -in < pkcs-token > -nocerts -out < key.pem >*"
4. Once you extract the private key, you need to upload the certificate on the Barracuda Web Application Firewall.

Uploading a Signed Certificate

You can upload a certificate either in PKCS#12 Token or PEM format. Perform the following steps to upload a certificate:

1. Go to the **BASIC > Certificates** page.
2. In the **Upload Certificate** section, specify a certificate name, select the certificate type (**PKCS12 Token** or **PEM Certificate**) and enter appropriate values in other fields.
3. Click **Upload Now**.

Uploading a Trusted Certificate

1. Go to the **BASIC > Certificates** page.
2. In the **Upload CA Certificate** section, specify a certificate name and select the CA certificate that you want to upload.
   Certificate should be uploaded in PEM (*.pem) format.
3. Click **Upload Now**.

Once a certificate is uploaded on the **BASIC > Certificates** page, it can be associated with the Services on the **BASIC > Services** page.