How to Configure Certificate Based Authentication for the Root User

https://campus.barracuda.com/doc/79463306/

Login and authentication of the administrative user *root* on a Barracuda CloudGen Firewall are processed using a two-factor authentication mechanism. The authenticity of the admin workstation is verified using a preferably encrypted certificate. In addition, the administrator has to authenticate himself or herself using a personal password. When creating new administrator profiles, Barracuda Networks recommends using certificates/keys instead of passwords whenever possible to avoid the exchange of security-relevant information when authenticating via public-key cryptography.

Certificates in PEM format cannot be used on Barracuda CloudGen Firewall systems.

Creating and Importing Certificates

Create a certificate on the Barracuda CloudGen Firewall using Barracuda Firewall Admin:

1. Open the **OPTIONS** tab in the top left corner of the screen and select **Settings**.
2. Expand the **Certificates and Private Keys** section.
3. Click **Create New Certificate/Key**.
4. Fill in the certificate details (e.g., Country, State, Name, Expiring date) and click **OK**.

The certificate is generated by using Microsoft Strong Cryptographic Provider v1.0 and can be imported from the Microsoft Certificate Management Store. It is displayed in the certificates list and provides key information in the **Hash** and **Public Key** column.

Configure Certificate Based Authentication

To configure certificate authentication for the *root* user, import the **root** public RSA key. If a key for automated SSH login is required, add it to the authorized root keys.

1. Go to **CONFIGURATION > Configuration Tree > Box > Administrative Settings**.
2. From the **Configuration Mode** menu, select **Switch to Advanced View**.
3. In the left navigation pane, click **Advanced System Access**.
4. Click **Lock**.
5. Select the **Authentication Mode** for system access.
6. Import the **Root Public RSA Key** for the *root* user.

7. In the **Authorized Root Keys** field, enter the public keys that are assigned to your *root* user in OpenSSH format, one key per line.
8. Click **Send Changes** and **Activate**.