Generating a Signed Certificate Using Let’s Encrypt

https://campus.barracuda.com/doc/84313865/

Let’s Encrypt is a certificate authority that provides free signed certificates that are valid for 90 days. The certificates are accepted by most of the browsers.

The Barracuda Web Application Firewall provides integration with Let’s Encrypt to generate, sign, install, and renew certificates for their domains running on the Barracuda Web Application Firewall.

- Let's Encrypt certificates can only be created by Local Users and Admins. Note that external users logged in from LDAP/Radius CANNOT create Let's Encrypt certificate.

- If the application has dual stack (both IPv4 and IPv6 services) then, Let's Encrypt always prefers the IPv6 address and challenge will be performed against IPv6 service. Hence in this case, Let's Encrypt certificate should always be generated for IPv6 service and not with IPv4 service.

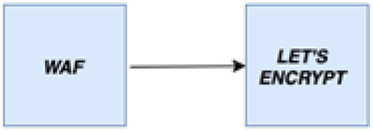
Before You Begin

- Create a HTTP service and also ensure that the service is in the **ACTIVE** mode.
- The backend server used by the HTTP service must respond **200 OK** for the Fully Qualified Domain Name (FQDN).
- Ensure that the FQDN can be resolved in an external DNS (e.g. Google 8.8.8.8) and the VIP for the HTTP service is accessible by the FQDN over the Internet on TCP port 80 (*IP Reputation policy must also not block the US*).
- Ensure that the FQDN can be resolved by the WAF and the management interface is also able to access the HTTP service on TCP port 80 (*If internal DNS points directly to the backend server add a Host Map entry for the FQDN and service VIP*).
- Ensure that the domain is accessible over the internet on TCP port 80.
- Ensure that the domain is accessible to the HTTP service that you created above.
- Allow outbound access to https://acme-v02.api.letsencrypt.org on the firewall.
- Ensure that the Public IP of the domain maps the barracuda service IP.
- Ensure that the "Allow Administration Access" for WAN is set to *Yes* for UI to successfully create a Let's Encrypt certificate.

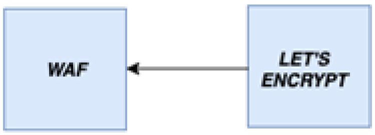
Refer to the following for more information on Let's encrypt:

- https://letsencrypt.org/how-it-works/
- https://letsencrypt.org/docs/integration-guide/

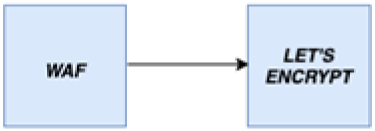
Certificate Generation – High level Flow



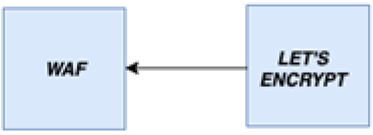
1. WAF sends a certificate sigining request(CSR) to Lets Encrypt for the desired domain.



2. Let's Encrypt receives WAF's certifcate signing request for the domain and sends a challenge to verify if the domain is valid



3. WAF receives challenge from Let's Encrypt, solves the challenge and send it back to Let's Encrypt for verification.



4. Let's Encrypt receives the solved challenge from WAF and it has been solved correctly it issues a signed certificate for the domain and the signed certificate is uploaded to the WAF

Challenges Initiated by the Let's Encrypt Service

Refer https://letsencrypt.org/docs/challenge-types/

The firmware handles the creation of the Allow Deny Rule and the corresponding Response page to make the challenge response available for the Let's Encrypt service. After the certificate is leased, these rules are removed from the system.

To generate the certificate from Let’s Encrypt CA:

1. Navigate to **BASIC > Certificates** and then click the **Let’s Encrypt** button from the **Certificate Generation** section. The **Get Certificate** from **Let's Encrypt** dialog box opens.

   If the **Use Let's Encrypt** button is not visible on the Certificate Generation section, please contact Barracuda Networks Technical Support for assistance.
2. Specify values for the following fields:
   1. **Certificate Name** - Enter a name to identify this certificate.
   2. **Key Type** - Select Key Type as RSA
   3. **Common Name** - Enter the domain name (DN) of the web server for which you want to generate the certificate. For example: "barracuda.domain.com".
   4. **Subject Alternative Names (SAN)** - Enter Subject Alternative Names (SAN) that needs to be associated with the certificate. Select DNS attribute from the drop-down list, and provide the appropriate value. For example: For DNS, the DNS domain name is specified. Example : barracuda.yourdomain.com.

      Number of SAN entries per certificate is limited to 99.
   5. **Services** - Click the drop-down list and then select the service on which this domain is listening . HTTP and HTTPS that have a redirect service will be listed here.
   6. **Renew Automatically** - Select Yes if you want the signed certificates to get automatically renewed after the validity period. Click the drop-down list and select the number of days after which you want the certificate to be renewed.

      Ensure that the HTTP service exists and is working in Active mode when you are performing an auto-renewal of the Let's Encrypt certificate.
3. Click **Generate Certificate** . You can view the created certificate in the **Saved Certificates** section.

Figures

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.