Client Certificate Validation Using OCSP and CRLs

https://campus.barracuda.com/doc/4259963/

The Barracuda Web Application Firewall supports Online Certificate Status Protocol (OCSP) and Certificate Revocation Lists (CRLs) to determine the current status of client digital certificates. SSL connections from clients can be allowed or blocked based on the status of the client certificate presented to the Barracuda Web Application Firewall, which is maintained externally by a certificate management system.

OCSP Validation	CRL Validation
The Barracuda Web Application Firewall connects to the certificate management system to verify the current status of a client certificate.	The certificate is verified using the downloaded CRL file.
OCSP provides current revocation status information for certificates.	Certificate Revocation Lists (CRLs) provide periodically updated certificate status.

Client Certificate Validation Using OCSP

When a client attempts to access a server over an SSL connection that requires client certificate, an OCSP status request for the client certificate is sent to an OCSP responder. The OCSP responder determines whether the status request contains the information required to identify the certificate and then returns a signed response message indicating one of the following:

- **GOOD** - a positive response indicating that the certificate has not been revoked.
- **REVOKED** - a negative response indicating that the certificate has been revoked.
- **UNKNOWN** - indication that the OCSP responder has no information about the requested certificate.

For any error or failure, the responder may return an unsigned message indicating a failed communication, logged under System Logs. Errors can occur because of a malformed request, an internal error, or an unauthorized request. To view system logs, navigate to the **ADVANCED > System Logs** page. If you want system events sent to the syslog servers, configure one or more (maximum of three) syslog servers using **Add Syslog Server** on the **ADVANCED > Export Logs > Syslog** section. For more information on configuring syslog, see How to Export Logs from the Barracuda Web Application Firewall.

Enforce Client Certificate must be set to **Yes** for a service on the **BASIC > Services** page if you want to authenticate client certificates using OCSP.

Configuring OCSP Validation

To enable OCSP validation, do the following:

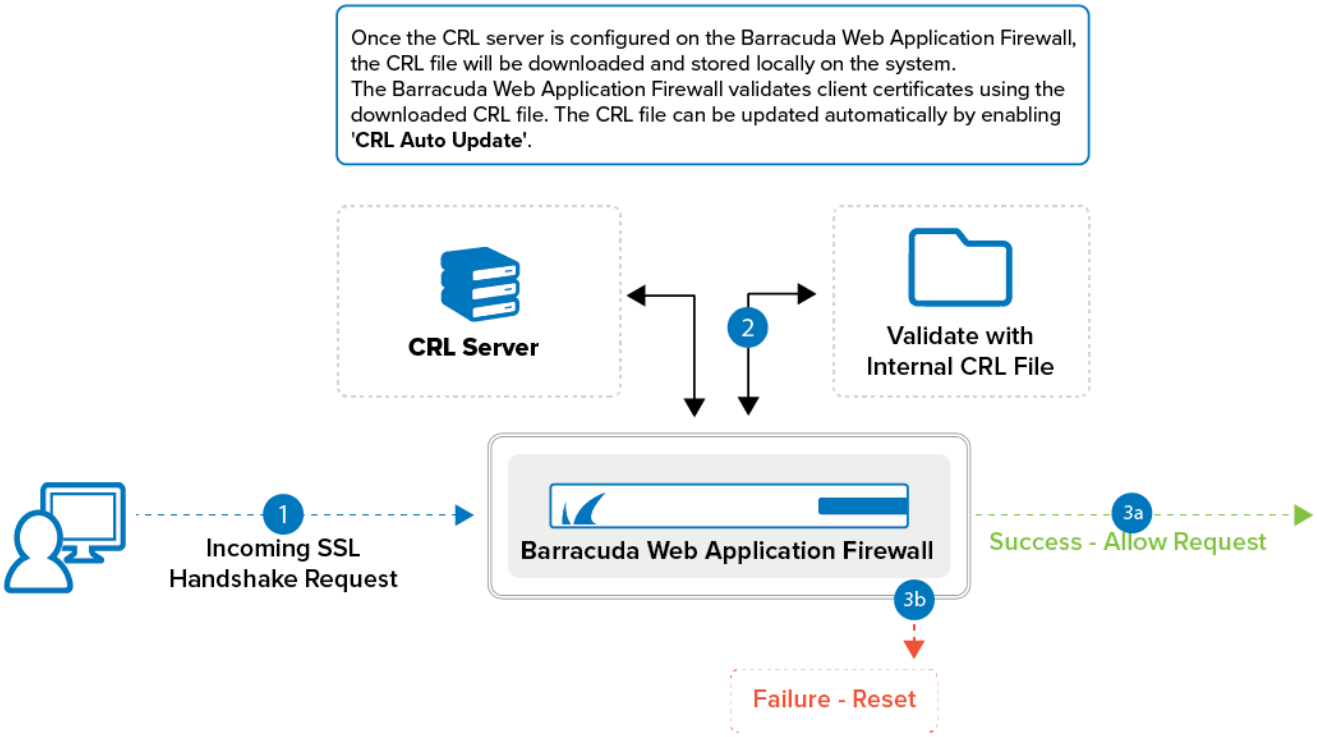
1. Go to the **ACCESS CONTROL > Client Certificates** page.
2. In the **Client Certificate Validation - OCSP** section, identify the service for which you want to enable client certificate validation using OCSP and click **Edit** next to that service. The **Client Certificate Validation - OCSP** window opens.
3. Specify values for the following fields:
   - **Enabled** – Set to **Yes** to enable OCSP validation.
   - **OCSP Responder URL**– Specify the OCSP responder URL. This is the URL issued by the trusted Certificate Authority (CA) where the Barracuda Web Application Firewall will send OCSP requests. Both HTTP and HTTPS (SSL/TLS) URLs can be specified. For example, `http://ocsp.example.com`
   - **Certificate**– Select a certificate from the list to verify the signature on the OCSP response.
4. Click **Save**.

Client Certificate Validation using CRLs

A CRL file contains a list of client certificates that are not expired, but are revoked by the Certificate Authority (CA) that issued the certificate. The certificate might be revoked for various reasons, such as the certificate was compromised by an unauthorized user, or the user no longer works for that company.

You can add multiple CRLs to a service. When a CRL is added, the CRL file is downloaded and stored locally on the Barracuda Web Application Firewall. This file remains in use unless automatic updates are configured. The CRL file can be updated periodically (daily, weekly, or monthly) by enabling the **CRL Auto Update** option. If CRL validation is enabled and a client attempts to access a server with a certificate, the Barracuda Web Application Firewall validates the certificate using the downloaded CRL file. If the certificate presented by the client matches a revoked client certificate in the CRL, the SSL connection from the client is dropped. Otherwise, the connection is established and the client is allowed to access the requested website. Also, if the CRL expires and there is no updated version available, the client authentication fails and the connection will be dropped.

If the certificate presented by the client contains the CRL path name in it, the Barracuda Web Application Firewall validates the CRL path name with the file name configured in the **CRL URL** parameter.



The Barracuda Web Application Firewall uses the default gateway or a static route to access the server hosting the CRL.

Configuring CRL Validation

To enable CRL validation, do the following:

1. Go to the **ACCESS CONTROL > Client Certificates** page.
2. In the **Client Certificate Validation - CRL** section, identify the service requiring client certificate validation using CRLs and click **Add** next to that service. The **Add CRL** window opens.
3. Specify values for the following fields:
   - **CRL Name** – Specify the name of the CRL file.
   - **Enable CRL** – Select **Yes** to use this CRL file to validate the client certificates.
   - **CRL URL** – Specify the location of the CRL file to download.
     As a best practice, use a unique account for this integration point and grant it the least level of privileges to access the CRL file. This account requires READ privileges for the CRL file For additional information, see Security for Integrating with Other Systems - Best Practices
   - **CRL Auto Update** – Select **Yes** if you wish to automatically update the CRL file (daily, weekly, or monthly).
   - **Number of Retries** – Specify the maximum number of times the Barracuda Web

Application Firewall can attempt to download the CRL file from the specified path before giving up.

4. Click **Save**.

Figures