Client Certificate Validation Using OCSP

https://campus.barracuda.com/doc/19333481/

The Barracuda Load Balancer ADC supports Online Certificate Status Protocol (OCSP) to determine updated status of a digital certificate. While Certificate Revocation Lists (CRLs) provide periodically updated certificate status, OCSP provides more current revocation status information for certificates. A central OCSP server (aka OCSP Responder), a trusted Certificate Authority (CA) itself, collects and updates CRLs from various Certificate Authority (CA) servers. When OCSP is enabled, the Barracuda Load Balancer ADC communicates with the OCSP server to validate the revocation status of client certificates before allowing or denying SSL connections from the respective clients.

Functioning of OCSP Validation

When a client attempts to access a server, an OCSP status request for the client certificate is sent to an OCSP Responder. The OCSP Responder validates whether the status request contains the information required to identify the certificate and then returns a signed response message indicating the status as one of the following:

- "**GOOD**" indicates a positive response that the certificate is not revoked.
- "**REVOKED**" indicates that the certificate has been revoked.
- "**UNKNOWN**" indicates 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 the Online help .

> **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 **TRAFFIC > Client Certificates** page.

2. In the **Client Certificate Validation - OCSP** section identify the Service for which you want to enable client certificate validation, and click **Edit** next to that Service. The **Client Certificate Validation - OCSP** window appears.
3. Specify values for the following fields:
    1. **Enabled** - Set to *Yes* to enable OCSP validation.
    2. **OCSP Responder URL** - Specify the OCSP Responder URL. This is the URL issued by the trusted Certificate Authority (CA) where the Barracuda Load Balancer ADC will send the OCSP requests. Both HTTP and HTTPS (SSL/TLS) URLs can be specified. For example, `http://ocsp.example.com`
    3. **Certificate** - Click the drop-down list and select the certificate to verify the signature on the OCSP response.
4. Click **Save Changes**.