Troubleshoot Error "517 Upstream Certificate Revoked"

Contents

Introduction

This document describes how to troubleshoot the error "517 Upstream Certificate Revoked" when browsing to an HTTPS url.

Issue

When the Umbrella Secure Web Gateway (SWG) web proxy is configured to perform HTTPS Inspection, a user can receive a **517 Upstream Certificate Revoked** error page. This error indicates that the requested website sent a digital certificate in the TLS negotiation which has a status of "revoked" according to the issuer of that certificate, or a similar authority. A revoked certificate is no longer valid.

Cause

When an Umbrella client makes an HTTPS request via the Umbrella Secure Web Gateway, SWG performs certificate revocation checks using the Online Certificate Status Protocol (OCSP). OCSP provides the revocation status of a certificate. SWG makes OCSP requests for certificate revocation status on behalf of the Umbrella clients.

SWG determines the certificate revocation status of the requested webserver's certificate and all issuing intermediate certificates in the path to a trusted root certificate. These checks ensure that a valid chain of trust has not become invalid since issuance.

In a digital certificate which uses OCSP revocation checking, the "Authority Information Access" X.509 extension contains one or more "OCSP" fields. A field contains an HTTP URL for an OCSP "endpoint" (webserver) which can be queried for the certificate's revocation status. SWG makes requests to each OCSP URL in a certificate until a response is received which indicates one of:

- the certificate is valid (not revoked) at which time SWG permits the web request to proceed, OR
- anything other than an OCSP "certificate valid" response (for example the certificate is revoked, the server cannot answer at the present time, an HTTP error status, a network/transport layer timeout, and so on) at which time SWG presents the appropriate error page/message and the web request fails

Note that OCSP responses are typically cached and used to respond to future checks. Caching time is set by the server in the OCSP response.

Different behavior when browsing directly

Web clients can use a variety of revocation checking mechanisms, depending on the client. For example, Google's Chrome browser does not use either the OCSP or the standard CRL methods, by default. Instead, Chrome uses a proprietary version of a CRL called CRLSet, which Secure Web Gateway does not use. As a result, Chrome might not produce the same result as SWG when checking a certificate's revocation status.

Note however that, as the CRLSet documentation states, "in some cases, the underlying system certificate library always performs these checks no matter what Chromium does." Thus, depending on your local environment, an OCSP and/or CRL check can be performed by either your browser, or the operating system’s cryptographic service libraries, such as SChannel, Secure Transport, or NSS.

Note also that OCSP and CRL checks are not guaranteed to produce the same result.

Consult your browser or operating system vendor's documentation to determine which certificate revocation checks are performed by your clients when browsing.

Resolution

Use of valid certificates is the responsibility of the webserver administrator. Remediation of revoked certificates must be performed on the server by the server administrator. Cisco Umbrella cannot assist in this process.

Cisco Umbrella strongly advises against accessing a website that uses a revoked certificate. Work-arounds can only be employed when the user fully understands why a site uses a revoked certificate, and fully accepts any risks.

To avoid the error, the site can be exempted from HTTPS Inspection by creating a Selective Decryption List that includes the site's domain name. The Selective Decryption List would be applied to the Web policy

which permits access to the site. Alternatively, the site can be added to the External Domains list to send traffic directly to the site, bypassing SWG.

Additional Information

Customers wishing to confirm whether a server's certificate is revoked can use third-party tools designed to check revocation status. Most notably, the Qualys SSL Labs' **SSL Server Test** tool performs both OCSP and CRL checks, in addition to providing other certificate validity information. The tool is available online at:

- https://www.ssllabs.com/ssltest/analyze.html

We recommend using this tool to check the site which produces a **517 Upstream Certificate Revoked** error, prior to opening a support case with Cisco Umbrella.

See also: https://support.umbrella.com/hc/en-us/articles/4406133198100-Certificate-and-TLS-Protocol-Errors