Troubleshoot Browswer Certificate Revocation Errors while Using Umbrella Filtering

Contents

Introduction

This document describes how to resolve browser certificate revocation errors while using Umbrella filtering.

Issue

When using Allow-Only Mode or restrictive Category Settings you often have to add several domains to the allow list in order for a site to load properly.

One specific problem is that Certificate Revocation Lists (CRLs) for HTTPS/SSL websites can be blocked, which in turn generates errors in some browsers. Sometimes blocking these CRLs also introduces latency whilst the browser tries to do its validation.

Cause

CRLs (Certificate Revocation Lists) and newer OCSP (Online Certificate Status Protocol) are used to ask a certificate authority whether an SSL certificate has been revoked for any reason. This typically happens transparently in the background when you are connecting to a HTTPS website.

The idea is that the browser stops the user going to the website if the certificate has been revoked in the event that the certificate / CA is compromised. It is a good idea to allow access to CRLs.

In Allow-Only Mode most CRLs are blocked unless you have specifically unblocked them. The impact of this depends on which web browser is being used...

- **Internet Explorer 7** shows a pop-up warning with an error such as the one below.

  > Revocation information for the security certificate for this site is not available.

- Later versions of **Internet Explorer** do not present any error unless a specific registry key flag has been set.
- **Google Chrome** shows a warning next to the address bar. Clicking on the warning shows this error:

  > Unable to check whether the certificate has been revoked

- **Firefox** does not present any error unless *security.OCSP.require* setting has been set in *about:config*

Resolution

1. Find the CRL for the certificate by viewing the certificate in your web browser (steps vary depending on browser).
2. Use the 'Details' tab and look for this information:
    - CRL Distribution Points
    - Authority Access Information
3. Note down the URL information (example below) and add these to the allow list on your Umbrella dashboard: