使用Umbrella过滤时排除浏览器证书吊销错误故障

目录

简介

本文档介绍在使用Umbrella过滤时如何解决浏览器证书吊销错误。

问题

使用仅允许模式或限制类别设置时，通常必须向允许列表中添加多个域，以便站点正确加载。

一个特定问题是，HTTPS/SSL网站的证书吊销列表(CRL)可能被阻止，这反过来会在某些浏览器中生成错误。有时，阻止这些CRL也会在浏览器尝试执行验证时导致延迟。

原因

CRL（证书撤销列表）和较新的OCSP（在线证书状态协议）用于询问证书颁发机构是否因任何原因撤销了SSL证书。 当您连接到HTTPS网站时，这通常在后台透明地发生。

其思路是，如果证书已被撤销，则浏览器会在证书/CA受到危害时阻止用户访问网站。 允许访问CRL是一个好主意。

在仅允许模式下，大多数CRL被阻止，除非您已明确取消阻止它们。 影响取决于所使用的Web浏览器……

- Internet Explorer 7显示一个弹出警告，显示如下所示的错误。 此网站的安全证书的吊销信息不可用。
- Internet Explorer的更高版本不会显示任何错误，除非已设置特定的注册表项标志。
- Google Chrome在地址栏旁边显示警告。 单击警告将显示以下错误： 无法检查证书是否已吊销
- 除非在about:config中设置了security.OCSP.require设置，否则Firefox不会显示错误

分辨率

1. 在Web浏览器中查看证书，查找证书的CRL（步骤因浏览器而异）。
2. 使用“详细信息”选项卡并查找以下信息：

- CRL分发点
- 权限访问信息

3. 记下URL信息（下面的示例），并将其添加到Umbrella控制面板上的允许列表：

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。