排除错误"517 Upstream Certificate Revoked"

目录

简介

本文档介绍在浏览到HTTPS URL时如何解决错误“517 Upstream Certificate Revoked”。

问题

当Umbrella安全Web网关(SWG)Web代理配置为执行HTTPS检查时，用户可以收到517 Upstream Certificate Revoked错误页面。此错误表示请求的网站在TLS协商中发送了一个数字证书，根据该证书的颁发者或类似颁发机构的状态，该数字证书的状态为“已撤销”。已撤销的证书不再有效。

13351060307092

原因

当Umbrella客户端通过Umbrella安全Web网关发出HTTPS请求时，SWG使用在线证书状态协议(OCSP)执行证书撤销检查。OCSP提供证书的撤销状态。SWG代表Umbrella客户端发出证书撤销状态的OCSP请求。

SWG确定所请求Web服务器的证书以及受信任根证书路径中所有颁发中间证书的证书撤销状态。这些检查可确保有效的信任链自颁发后未变为无效。

在使用OCSP撤销检查的数字证书中，“Authority Information Access” X.509扩展名包含一个或多个“OCSP”字段。字段包含可查询证书撤销状态的OCSP“终端”（Web服务器）的HTTP URL。SWG向证书中的每个OCSP URL发出请求，直到收到指示以下各项之一的响应：

- 证书有效（未撤销），此时SWG允许Web请求继续，或者
- 除OCSP“证书有效”响应（例如，证书被吊销、服务器当前无法应答、HTTP错误状态、网络/传输层超时等）之外，其他任何响应，在这时SWG显示相应的错误页面/消息，并且Web请求失败

请注意，OCSP响应通常缓存并用于响应将来的检查。缓存时间由服务器在OCSP响应中设置。

直接浏览时的行为不同

Web客户端可以使用各种撤销检查机制，具体取决于客户端。例如，默认情况下，Google的Chrome浏览器不使用OCSP或标准CRL方法。相反，Chrome使用名为CRLSet的CRL的专有版本，安全Web网关不使用此版本。因此，Chrome在检查证书的撤销状态时可能不会产生与SWG相同的结果。

但请注意，如CRLSet文档所述，“在某些情况下，无论Chromium做了什么，基础系统证书库始终会执行这些检查。” 因此，根据您的本地环境，OCSP和/或CRL检查可由您的浏览器或操作系统的加密服务库（如SChannel、安全传输或NSS）执行。

另请注意，OCSP和CRL检查不能保证产生相同的结果。

请参阅浏览器或操作系统供应商的文档，以确定您的客户端在浏览时执行哪些证书撤销检查。

分辨率

使用有效证书是Web服务器管理员的责任。必须由服务器管理员在服务器上执行已撤销证书的补救。Cisco Umbrella无法协助此过程。

Cisco Umbrella强烈建议不要访问使用已撤销证书的网站。只有在用户完全了解站点使用撤销证书的原因并完全接受任何风险时，才能使用解决方法。

为避免此错误，可以通过创建包含站点域名的选择性解密列表来免除站点的HTTPS检查。“选择性解密列表”(Selective Decryption List)将应用于允许访问该网站的Web策略。或者，可以将该站点添加到外部域列表，以绕过SWG直接将流量发送到该站点。

Additional Information

希望确认服务器证书是否已撤销的客户可以使用旨在检查撤销状态的第三方工具。最值得注意的是，Qualys SSL Labs的SSL Server Test工具除了提供其他证书有效性信息外，还执行OCSP和CRL检查。该工具可在以下网址在线获得：

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

我们建议使用此工具检查产生517 Upstream Certificate Revoked错误的站点，然后再使用Cisco Umbrella打开支持案例。

另请参阅：https://support.umbrella.com/hc/en-us/articles/4406133198100-Certificate-and-TLS-Protocol-Errors

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）。