解决516上游证书CN不匹配错误

目录

简介

本文档介绍如何解决516上游证书CN不匹配错误。

问题

当将Umbrella安全Web网关(SWG)代理配置为执行HTTPS检查时，用户在使用HTTPS URL浏览到网站时可能会收到516 Upstream Certificate CN Mismatch错误页面。

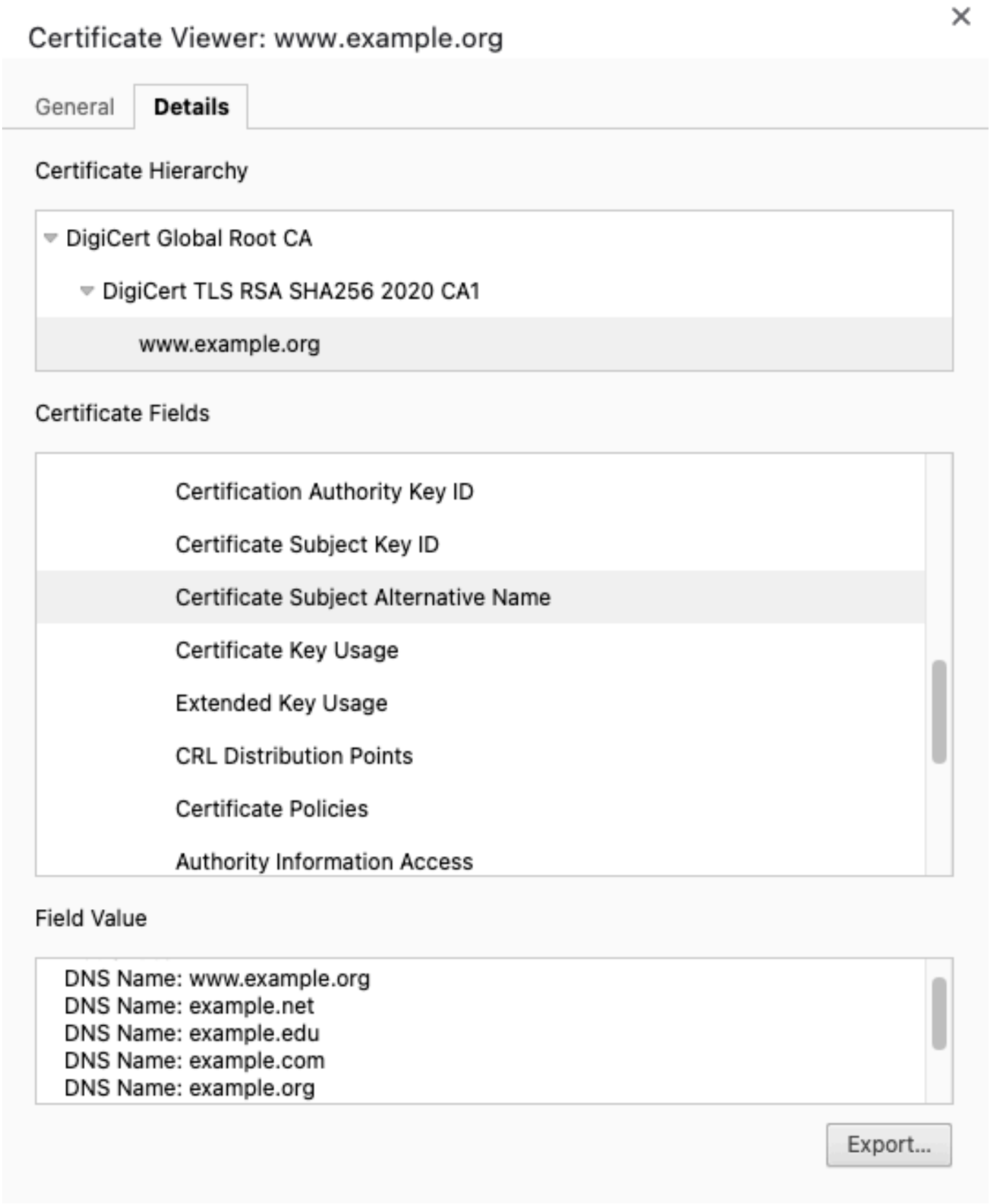
此错误不表示网站证书的Subject字段中的Common Name(CN)属性有问题。相反，此问题涉及证书的使用者备用名称(SAN)扩展中的DNS名称属性。

在阅读本文后，如果您无法确定516错误页的原因，请与Umbrella技术支持联系，并向我们提供本文档证书身份错误部分中指定的信息。

证书身份机制

当请求HTTPS URL时，浏览器或其他Web客户端通过TLS协商的Client Hello消息中的Server Name Indication(SNI)扩展将URL中的域名发送到Web服务器。服务器使用此SNI值选择要返回到客户端的服务器证书，因为服务器通常托管多个网站，并且可能为部分或所有站点拥有不同的证书。

当Web客户端收到服务器证书时，客户端通过将请求的域名与证书的Subject Alternative Names扩展的DNS Name属性中的域名进行比较，来验证证书是否是请求的正确证书。此图显示服务器证书中的这些SAN。



16796247745556

此Web服务器返回此证书，以响应具有这些SNI值的请求，以及字段值面板中不可见的其他请求：

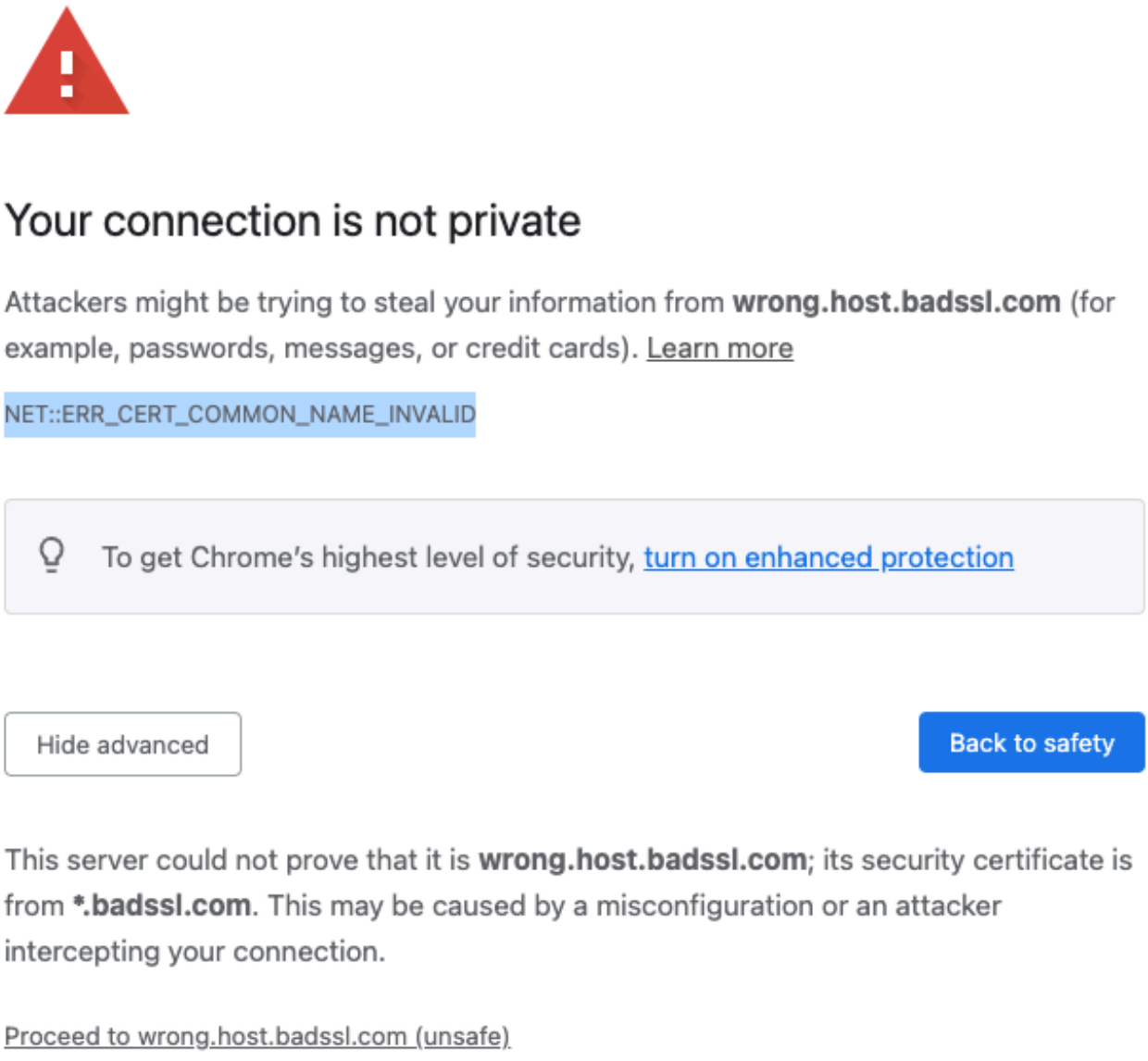
- www.example.org
- example.net

- example.edu
- example.com
- example.org

请注意，SAN "example.com"与"www.example.com"的SNI不匹配。 但是，“*.example.com”的通配符SAN会匹配“www.example.com”的SNI或包含单个标签（不带“。”的字符串）的任何其他域名。字符)预置到example.com，但不包含多个标签。例如，“www.hr.example.com”与“*.example.com”不匹配，因为“www.hr”由两个标签组成：“www”和“hr”。单个通配符只能匹配单个标签。

证书身份错误

当Web客户端收到服务器证书时，如果SAN的DNS名称与所请求的URL中的域名中的SNI不匹配，则Web客户端通常会向用户显示错误。此图像显示Chrome显示“NET::ERR_CERT_COMMON_NAME_INVALID”间隙页面。



在映像中，请求的站点为“https://wrong.host.badssl.com”，该站点与任何SAN都不匹配。证书包含通配符SAN DNS名称“*.badssl.com”，其通配符只能匹配单个标签，如“host”。 此外，证书没有精确值为“wrong.host.badssl.com”的SAN DNS名称或通配符SAN “*.host.badssl.com”，因此用户出现此错误。

要确定证书身份不匹配的原因，请使用浏览器的证书查看功能检查证书的SAN DNS名称，并与所请求URL中的域名进行比较。或者，可以使用Qualys SSL Server Test等工具诊断证书身份问题。

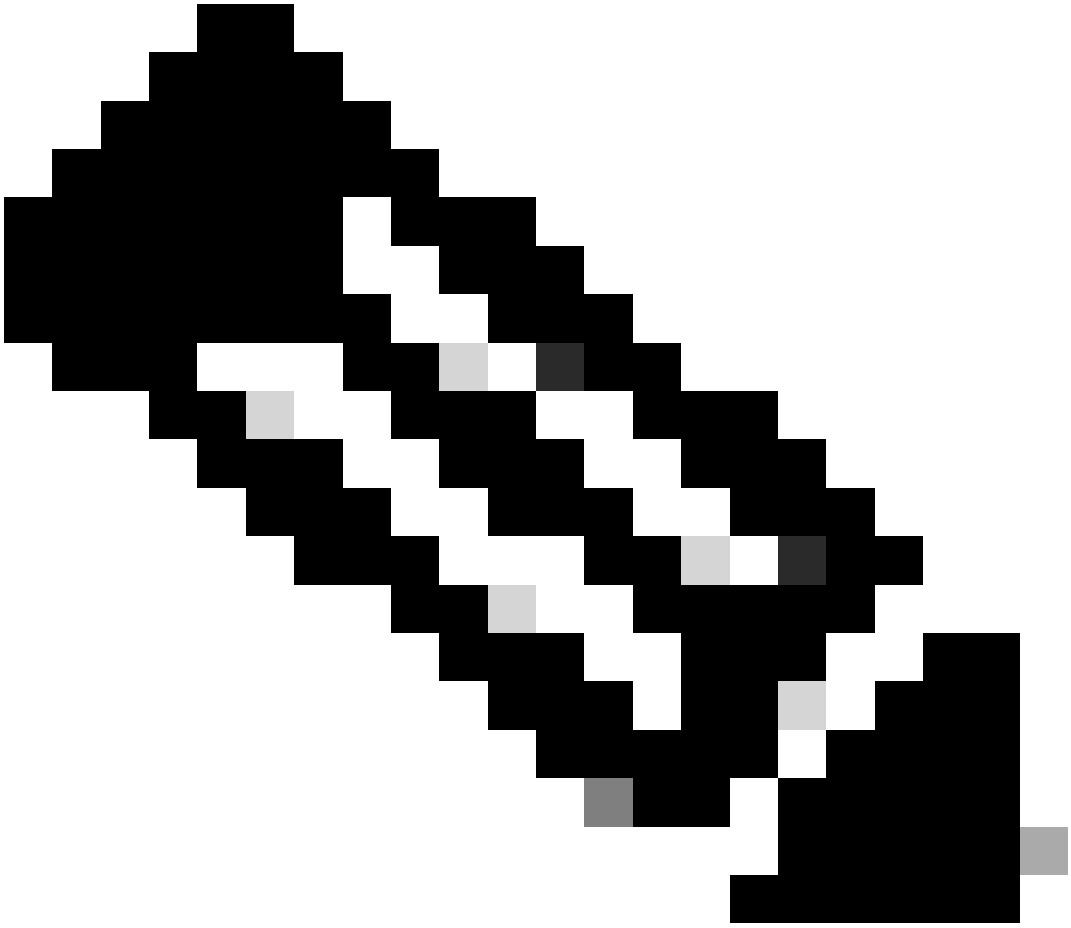
如果在采用本节中的信息后无法确定516错误的原因，或者无法采用下一部分中的解决方案和解决方法，请通过Umbrella技术支持打开案例并提供：

1. 截图
    - 浏览器的地址栏显示请求的URL
    - 整个516错误页面（请参见下一节中的图像）
2. 从地址栏复制的URL文本

分辨率

要解决此问题，请使用与证书中的某个SAN DNS名称匹配的域名访问服务器。这可能需要网站管理员将匹配的域名添加到区域的DNS中。或者，管理员可以重新颁发证书以将URL的域名包含在一个SAN DNS名称中。

作为解决方法，可以将URL的域名添加到安全Web网关代理的选择性解密列表或智能代理中的目标列表。将列表应用于相应的Web策略规则集设置（安全Web网关）或DNS策略允许列表（智能代理）。 这可以防止对网站的请求被代理解密，从而防止代理显示516错误页面。



注意：不支持同时使用安全Web网关代理和智能代理。每个组织只能采用一种代理技术。建议订用安全Web网关的组织使用SWG，而不使用智能代理。

公用名已弃用

Web客户端最初将所请求URL中的域名与证书的Subject字段中的Common Name(CN)属性进行匹配。这种机制在现代Web客户端中已过时；现在，域与Subject Alternative Name扩展的DNS Names匹配。但是，错误消息文本通常继续引用已弃用的机制，例如Chrome中的“NET::ERR_CERT_COMMON_NAME_INVALID”。

同样，当SWG代理从Web服务器请求URL时，Umbrella SWG会显示516错误页面，并显示以下文本，并且会出现SAN DNS名称不匹配的情况：

16794325789332

Cisco Umbrella计划在未来更新此文本，以更好地反映当前行为。

Additional Information

请参阅RFC 5280:Internet X.509公钥基础设施证书和证书撤销列表(CRL)配置文件，第4.1.2.6节（有关证书主题的信息）和第4.2.1.6节(有关主题备用名称)。

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）。